



**NAMIBIA UNIVERSITY**  
**OF SCIENCE AND TECHNOLOGY**

**Faculty of Computing and Informatics**  
**Department of Informatics**

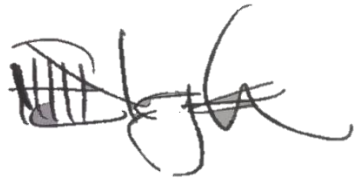
**A SECURE FRAMEWORK FOR CLOUD-BASED COMPUTING SERVICE  
ADOPTION IN THE NAMIBIAN GOVERNMENT SECTOR**

Thesis submitted in partial fulfilment of the requirements for the degree of  
**Master of Informatics**  
at the  
Namibia University of Science and Technology

<b>Presented by:</b>	<b>Eunike Ndahambelela Nghihalwa</b>
<b>Student Number:</b>	<b>200866907</b>
<b>Supervisor:</b>	<b>Dr Fungai Bhunu Shava</b>
<b>Co-Supervisor:</b>	<b>N/A</b>
<b>Submission Date:</b>	<b>31 January 2019</b>

## DECLARATION

I, Eunike Ndahambelela Nghihalwa, born on 8 August 1989 at Omafo, Namibia, hereby declare that the work contained in the report presented for the degree of the Master of Informatics at the Namibia University of Science and Technology, entitled: **“A secure framework for cloud-based computing services adoption in the Namibian government sector”** is my original work, and that I have not previously, in its entirety or in part, submitted it to any other university or higher education institution for the award of a degree.



Eunike N. Nghihalwa

20 March 2019

Date

## **DEDICATION**

This thesis is dedicated to the loving memory of my late grandmother, Frieda Naufiku Efraim Hamatundu, for having believed that I can achieve greater things in life.

## **ACKNOWLEDGEMENTS**

Firstly, I would like to thank the Almighty God, who made this research possible and his massive guidance throughout my academic years. Secondly, my wholehearted appreciation goes to my family and friends, especially my mom, Mrs Sylvia Hausholo, for their unwavering support and encouragement during my study years. Mom, your unconditional love has been my pillar of my strength during my academic years.

Thirdly, special thanks to my supervisor, Dr Fungai Bhunu Shava for your academic guidance, continuous support and perseverance during my study. I am indebted and delighted that you have been part of my academic journey. I could not have made it this far without your guidance. I appreciate every effort.

Fourthly, I would like to express my humble gratitude to Mr. E. Nafele, Mr. E. Titus, Mr. P. Van Heerden and Mr L. Maruwasa for their guidance and willingness to share their vast knowledge during this research and write up of my thesis. To my best friend Taneni, thank you for your continuous support and encouragement.

Lastly, a special token of appreciation goes to the IT departments of the Office of the Prime Minister, Ministry of Urban and Rural Development, all 14 regional councils, including decentralised functions and the expert review participants. Your prompt contribution made this study a success. I would also like to thank all the other individuals and institutions, whose names have not been mentioned above for their contributions towards my thesis.

## **PUBLICATIONS**

Nghihalwa, E., & Bhunu Shava, F. (2018). An assessment of cloud computing readiness in the Namibian government's Information Technology Departments. Melecon '18 (pp. 92-97). Marakash: IEEE .

Nghihalwa, E., & Bhunu Shava, F (2018). A Secure Cloud Adoption Framework (SCAF) for the Namibian government information technology departments. 2nd World Conference on Smart Trends in System, Security, Security & Sustainability. London. doi:10.1109/WorldS4.2018.8611573.

## **ABSTRACT**

The term cloud computing is derived from the cloud diagram on the network that represented the Internet for years until a variety of services emerged that allowed computing resources to be accessed over the Internet. The technology extends existing IT capabilities without spending much on new information technology (IT) infrastructure, training new staff and software licence. Case studies from the United States, Europe, Africa and Asia governments' spectacle cloud adoption services across the public sector. Cloud is increasingly trending and more and more organisations are making use of it. Despite the latest advances, some companies are still reluctant to migrate because of the paradigm security issues and challenges. IT infrastructure is difficult to maintain, outsourcing of expertise and tedious infrastructural procurement processes are problems experienced by Namibian government IT departments. Hence, the motive to assess and analyse cloud computing for future IT infrastructure and security issues and challenges for adopting cloud-based Infrastructure as a Service (IaaS) in the Namibian government institutions. This research presents a proposal on a secure framework for cloud-based adoption in the Namibian government sector, which is a case study of the Office of the Prime Minister (OPM) and Ministry of Urban and Rural Development (MURD) IT department. A qualitative case study research approach using the design science research paradigm was used to address the research objectives. Data was collected using interviews, online questionnaires, literature review and experts review. Design science research was used to come up with the framework. The study identified four main factors essential for cloud adoption: organisational factors, technological enablers, environmental factors and user characteristics. The study further elaborated on the components and the factors that mitigate security risks such as service configuration, security management, trust management, service monitoring, confidentiality, authentication, policies and an integrated cloud security architecture that can satisfy cloud security. Experts in the field of information technology and security reviewed the framework and their feedback informed the refinement of the artefact. The findings will contribute to Namibia's Vision 2030 strategy and new technology horizon of Namibia's future IT cloud infrastructure. The framework is a guideline on how the Namibian government can securely position itself to the cloud computing paradigm, increase and promote service delivery among the 14 regional offices around Namibia with a centralised resources management system, save costs, and promote effective and efficient work

productivity. Finally, the framework could assist the Namibian government management to make informed decisions.

***Keywords: adoption, cloud computing, framework, government***

## TABLE OF CONTENTS

DECLARATION.....	i
DEDICATION.....	ii
ACKNOWLEDGEMENTS.....	iii
PUBLICATIONS .....	iv
ABSTRACT .....	v
TABLE OF CONTENTS.....	vii
LIST OF FIGURES .....	xiv
LIST OF TABLES .....	xv
ABBREVIATIONS/ACRONYMS.....	xvii
CHAPTER 1: INTRODUCTION .....	1
1.1 Background.....	1
1.2 The status of IT departments in the Namibian government .....	4
1.3 Statement of the problem.....	4
1.4 Aim.....	5
1.5 Research questions and objectives .....	5
1.6 Significance of the study .....	5
1.7 Limitations .....	6
1.8 Chapter outline .....	6
CHAPTER 2: LITERATURE REVIEW .....	8
2.1 Introduction .....	8
2.2 Cloud Computing Characteristics .....	9
2.3 Cloud Computing Benefits .....	10
2.4 Cloud Computing in Government .....	13
2.4.1 Case Studies of Cloud Computing Adoption in Government .....	15
2.4.1.1 South Africa.....	15
2.4.1.2 United States Government .....	16



2.4.1.3	European Government .....	17
2.4.1.4	Asian Government .....	17
2.5	Cloud Computing Security Issues and Challenges.....	19
2.5.1	Confidentiality .....	19
2.5.2	Integrity.....	20
2.5.3	Availability.....	20
2.5.4	Network security attackers.....	21
2.5.5	Security.....	22
2.5.6	Cloud security solutions.....	23
2.6	Technology adoption overview .....	25
2.7	Frameworks .....	26
2.7.1	Existing Frameworks in Cloud Computing Adoption.....	26
2.7.1.1	A framework for secure cloud computing .....	26
2.7.1.2	A security framework in cloud computing infrastructure .....	27
2.7.1.3	Security framework for governmental cloud .....	29
2.7.1.4	Control framework for information and related technology .....	31
2.7.1.5	A decision framework for cloud computing .....	32
2.8	Chapter Summary .....	32
<b>CHAPTER 3: METHODOLOGY .....</b>		<b>35</b>
3.1	Introduction .....	35
3.2	Research Strategy.....	35
3.3	Design Science Research Strategy Overview .....	36
3.3.1	Mapping DSR characteristics with research objectives .....	39
3.3.2	Quality of the framework .....	43
3.3.3	Validity and Reliability .....	43
3.4	Data Triangulation .....	44
3.5	Data Collection .....	45

3.5.1	Primary data.....	46
3.5.1.1	Questionnaire .....	46
3.5.1.2	Interviews.....	47
3.5.2	Secondary data .....	48
3.5.2.1	Literature review, documentation and government publication.....	48
3.6	Sampling.....	48
3.7	Data Analysis .....	49
3.8	Unit Analysis .....	51
3.9	Research Ethics.....	52
3.10	Anonymity and Confidentiality .....	52
3.11	Chapter Summary .....	52
<b>CHAPTER 4: CASE STUDY .....</b>		<b>54</b>
4.1	Introduction .....	54
4.2	Case Studies Overview .....	55
4.3	Case Studies .....	55
4.3.1	Office of the Prime Minister.....	56
4.3.2	Ministry of Urban and Rural Development .....	60
4.4	Case Study Design .....	63
4.5	Demographic Results .....	65
4.5.1	Sample institutions.....	65
4.5.2	Portfolios of respondents .....	65
4.6	Perceived importance of Infrastructure as a Service and Software as a Service	66
4.7	Cloud Benefits.....	69
4.7.1	Perceived Cloud Benefits Over Traditional IT Infrastructure.....	70
4.7.2	Importance of cloud benefits.....	71

<b>4.8</b>	<b>Cloud Security and Other Related Issues .....</b>	<b>74</b>
<b>4.9</b>	<b>Challenges Hindering the Adoption of Cloud Computing by Namibian Government IT Departments.....</b>	<b>75</b>
<b>4.10</b>	<b>Security Concerns as a Stumbling Block for Cloud computing.....</b>	<b>75</b>
<b>4.11</b>	<b>Service Delivery and Accessibility Concerns .....</b>	<b>76</b>
<b>4.12</b>	<b>Interviews .....</b>	<b>77</b>
<b>4.12.1</b>	<b>Maximize Service Delivery .....</b>	<b>78</b>
<b>4.12.2</b>	<b>Main Cloud Challenges .....</b>	<b>79</b>
<b>4.12.3</b>	<b>Trust of cloud providers .....</b>	<b>80</b>
<b>4.12.4</b>	<b>Security Risks .....</b>	<b>81</b>
<b>4.12.5</b>	<b>Cloud Computing as a Future IT Model .....</b>	<b>82</b>
<b>4.12.6</b>	<b>Future Recommendations for Namibian Government Cloud Adoption</b>	<b>83</b>
<b>4.12.7</b>	<b>IT Policies and Regulations towards Cloud Adoption in Namibian Government IT Departments.....</b>	<b>83</b>
<b>4.12.8</b>	<b>Cloud Infrastructure Governance in Namibian Government IT Departments.....</b>	<b>84</b>
<b>4.13</b>	<b>Chapter Summary .....</b>	<b>84</b>
<b>CHAPTER 5: CASE STUDY FINDINGS, ANALYSIS AND DISCUSSIONS ...</b>		<b>85</b>
<b>5.1</b>	<b>Introduction .....</b>	<b>85</b>
<b>5.2</b>	<b>Demographic characteristics of the respondents.....</b>	<b>85</b>
<b>5.3</b>	<b>Benefits of Cloud Computing .....</b>	<b>88</b>
<b>5.3.1</b>	<b>Perceived cloud computing benefits .....</b>	<b>88</b>
<b>5.3.2</b>	<b>Perceived importance of cloud computing benefits .....</b>	<b>89</b>
<b>5.3.3</b>	<b>Benefits summary.....</b>	<b>91</b>
<b>5.4</b>	<b>Issues affecting cloud based infrastructure.....</b>	<b>93</b>

5.4.1	Cloud security and other related issues .....	93
5.4.2	Challenges hindering cloud computing adoption.....	95
5.5	Factors influencing cloud computing adoption .....	97
5.5.1	Organisational factors .....	97
5.5.1.1	Needs Assessment .....	98
5.5.1.2	Benefits .....	98
5.5.1.3	Executive management buy-in .....	98
5.5.1.4	Budget .....	99
5.5.1.5	Information security .....	99
5.5.1.6	Governance .....	99
5.5.1.7	Skills .....	100
5.5.1.8	Performance.....	100
5.5.2	Technological enablers .....	100
5.5.2.1	Infrastructure readiness .....	100
5.5.2.2	Compatibility .....	101
5.5.2.3	Security and privacy .....	101
5.5.2.4	Challenges .....	101
5.5.2.5	Service delivery.....	101
5.5.3	Environmental factors .....	102
5.5.3.1	Policies and regulations .....	102
5.5.3.2	Service providers .....	102
5.5.3.3	Information security .....	102
5.5.4	Users' characteristics .....	103
5.5.4.1	Awareness, knowledge and skills.....	103
5.5.4.2	Acceptance .....	103
5.6	Chapter summary .....	104
<b>CHAPTER 6: FRAMEWORK DESIGN PROCESS.....</b>		<b>108</b>
6.1	Introduction .....	108
6.2	Framework design.....	109
6.2.1	Framework Design Methodology.....	109

6.2.2	PHASE 1: Identify problem and motivate.....	110
6.2.3	PHASE 2: Define objectives of solutions.....	111
6.2.4	PHASE 3: Design and develop.....	112
6.2.4.1	Components identification.....	112
6.2.4.2	Component validation.....	115
6.2.4.3	Construct Relationship.....	117
6.2.4.4	Tentative design.....	121
6.2.4.5	Framework consolidation.....	123
6.2.5	PHASE 4: Theoretical Demonstration.....	126
6.2.6	PHASE 5: Framework evaluation.....	135
6.2.6.1	Expert Reviews.....	136
6.2.6.2	Framework evaluation tool.....	138
6.2.6.3	Data Analysis.....	138
6.2.6.4	Evaluation Findings.....	138
6.2.6.5	Conclusion remarks.....	150
6.2.6.6	Refined Framework.....	152
6.2.7	PHASE 6: Communication.....	155
6.3	Chapter summary.....	155
CHAPTER 7: RECOMMENDATIONS AND CONCLUSION.....		156
7.1	Introduction.....	156
7.2	Research contributions.....	157
7.3	Reflection.....	158
7.3.1	Scientific reflection.....	158
7.3.2	Methodological reflection.....	158
7.3.3	Substantive reflection.....	159
7.4	Lessons learnt.....	160
7.5	Research limitations.....	161
7.6	Future considerations.....	161

<b>7.7</b>	<b>Concluding remarks .....</b>	<b>162</b>
	<b>REFERENCES .....</b>	<b>165</b>
	<b>APPENDICES .....</b>	<b>176</b>
	<b>Appendix A: Permission Letter .....</b>	<b>176</b>
	<b>Appendix B: Approval Letter .....</b>	<b>177</b>
	<b>Appendix C: Cover Letter .....</b>	<b>178</b>
	<b>Appendix D: Publications .....</b>	<b>179</b>
	<b>Appendix E: Questionnaire .....</b>	<b>192</b>
	<b>Appendix F: Interview .....</b>	<b>196</b>
	<b>Appendix G: Framework Evaluation tool .....</b>	<b>197</b>
	<b>Appendix H: Language Editor’s Letter .....</b>	<b>213</b>

## LIST OF FIGURES

FIGURE 1-1: RESEARCH OUTLINE.....	7
FIGURE 2-1: CHARACTERISTICS OF CLOUD COMPUTING.....	9
FIGURE 2-2: A FRAMEWORK FOR SECURE CLOUD COMPUTING .....	27
FIGURE 3-1: DESIGN SCIENCE RESEARCH GUIDELINES .....	39
FIGURE 3-2: DATA SOURCE TRIANGULATION.....	45
FIGURE 3-3: DATA COLLECTION METHODS.....	46
FIGURE 4-1: ASSOCIATION OF CASES.....	55
FIGURE 4-2: OPM IT DEPARTMENTAL STRUCTURE .....	57
FIGURE 4-3: MURD IT DEPARTMENT STRUCTURE .....	61
FIGURE 4-4: SAMPLED GOVERNMENT INSTITUTIONS .....	65
FIGURE 4-5: RESPONDENTS' PORTFOLIOS.....	66
FIGURE 4-6: IMPORTANCE OF CLOUD BENEFITS.....	73
FIGURE 4-7: SECURITY AS A STUMBLING BLOCK TO CLOUD .....	76
FIGURE 6-1: FRAMEWORK STRUCTURE .....	109
FIGURE 6-2: FRAMEWORK DESIGN PROCESS .....	110
FIGURE 6-3: PROBLEMS FACED BY THE NAMIBIAN GOVERNMENT IT DEPARTMENTS .....	111
FIGURE 6-4: COMPONENTS IDENTIFIED FROM DATA SOURCES.....	112
FIGURE 6-5: SECURITY MITIGATIONS.....	117
FIGURE 6-6: CONSTRUCT OVERALL INTERRELATIONSHIPS .....	118
FIGURE 6-7: COMPONENTS RELATIONSHIP .....	119
FIGURE 6-8: CONCEPTUAL DESIGN .....	122
FIGURE 6-9: COMPOSITION OF ALL COMPONENTS .....	124
FIGURE 6-10: A SECURE CLOUD ADOPTION FRAMEWORK.....	125
FIGURE 6-11: CLOUD SERVICES MONITORING EVENTS.....	134
FIGURE 6-12: CLOUD SERVICES AUDITING .....	135
FIGURE 6-13: CHANGE MANAGEMENT.....	135
FIGURE 6-14: REFINED SECURE CLOUD ADOPTION FRAMEWORK .....	154
FIGURE 0-1: SECURE CLOUD ADOPTION FRAMEWORK.....	199

## LIST OF TABLES

TABLE 2-1: CLOUD SECURITY SOLUTIONS.....	24
TABLE 2-2: PLAN-DO-CHECK-ACT LIFECYCLE.....	30
TABLE 3-1: DESIGN SCIENCE RESEARCH ELEMENTS .....	38
TABLE 3-2: FRAMEWORK COMPONENTS.....	41
TABLE 3-3: DATA ANALYSIS PROCESS.....	50
TABLE 3-4: RESEARCH METHODOLOGY SUMMARY .....	52
TABLE 3-5: RESEARCH OBJECTIVE AND DATA COLLECTION TOOLS USED.....	53
TABLE 4-1: CLOUD COMPUTING FAMILIARISATION .....	67
TABLE 4-2: PERCEIVED IMPORTANCE OF IAAS AND SAAS TO NAMIBIA.....	68
TABLE 4-3: COMMENTS FROM RESPONDENTS .....	69
TABLE 4-4: PERCEIVED CLOUD BENEFITS OVER CURRENT IT WIRED INFRASTRUCTURE .....	71
TABLE 4-5: MAIN CONCERNS REGARDING THE USE OF CLOUD COMPUTING .....	74
TABLE 4-6: CHALLENGES HINDERING CLOUD ADOPTION .....	75
TABLE 4-7: SERVICE DELIVERY AND ACCESSIBILITY .....	76
TABLE 4-8: INTERVIEW QUESTIONS .....	77
TABLE 4-9: MAXIMIZE SERVICE DELIVERY AND SOLVE BACKLOG PROBLEMS.....	78
TABLE 4-10: MAIN CLOUD ADOPTION CHALLENGES IN THE NAMIBIAN IT ENVIRONMENT.....	79
TABLE 4-11: WHERE SHOULD SENSITIVE DATA BE STORED.....	80
TABLE 4-12: CAN WE TRUST CLOUD PROVIDERS WITH GOVERNMENT SENSITIVE DATA.....	80
TABLE 4-13: SECURITY RISKS .....	81
TABLE 4-14: CLOUD COMPUTING AS A FUTURE IT MODEL .....	82
TABLE 4-15 RECOMMENDATIONS FOR NAMIBIAN GOVERNMENT CLOUD ADOPTION.....	83
TABLE 4-16: SUGGESTED CLOUD IT POLICIES AND REGULATIONS.....	83
TABLE 4-17: WHO SHOULD GOVERN CLOUD INFRASTRUCTURE.....	84
TABLE 5-1: BEST CLOUD COMPUTING BENEFITS .....	92
TABLE 5-2: BEST CLOUD COMPUTING BENEFITS .....	104
TABLE 5-3: SECURITY ISSUES AND CHALLENGES AFFECTING CLOUD COMPUTING .....	105
TABLE 6-1: IDENTIFIED FRAMEWORK COMPONENTS.....	113
TABLE 6-2: GUIDELINES OF THE FRAMEWORK .....	122
TABLE 6-3: CLOUD COMPUTING ADOPTION TEAM ROLES DEFINED.....	126
TABLE 6-4: FACTORS AFFECTING CLOUD ADOPTION.....	127
TABLE 6-5: PARTICIPANTS' PROFILE.....	136
TABLE 6-6: EXPERT PROFILES.....	138



<b>TABLE 6-7: RELEVANCE OF CLOUD COMPUTING BENEFITS .....</b>	<b>140</b>
<b>TABLE 6-8: RELEVANCE OF CLOUD COMPUTING BENEFITS .....</b>	<b>140</b>
<b>TABLE 6-9: IMPORTANCE OF CLOUD COMPUTING BENEFITS .....</b>	<b>141</b>
<b>TABLE 6-10: RELEVANCE OF CLOUD COMPUTING CHALLENGES.....</b>	<b>142</b>
<b>TABLE 6-11: CLOUD ADOPTION COST EFFECTIVENESS.....</b>	<b>143</b>
<b>TABLE 6-12: PERFORMANCE RELEVANCE .....</b>	<b>144</b>
<b>TABLE 6-13: PERCEIVED USEFULNESS.....</b>	<b>144</b>
<b>TABLE 6-14: PERCEIVED EASE OF USE .....</b>	<b>145</b>
<b>TABLE 6-15: SECURITY CONTROLS.....</b>	<b>145</b>
<b>TABLE 6-16: IMPORTANCE OF POLICIES AND REGULATIONS .....</b>	<b>146</b>
<b>TABLE 6-17: IMPORTANCE OF GOVERNANCE TOWARDS CLOUD ADOPTION .....</b>	<b>146</b>
<b>TABLE 6-18: IMPORTANCE OF COMPLIANCE FACTORS .....</b>	<b>148</b>
<b>TABLE 6-19: RELEVANCE OF TECHNOLOGY READINESS.....</b>	<b>149</b>
<b>TABLE 6-20: OVERALL FRAMEWORK PERFORMANCE.....</b>	<b>149</b>
<b>TABLE 6-21: FRAMEWORK EVALUATION DEVELOPMENT PROCESS .....</b>	<b>152</b>
<b>TABLE 7-1: RESEARCH QUESTION, ANSWERS AND EVIDENCE .....</b>	<b>162</b>

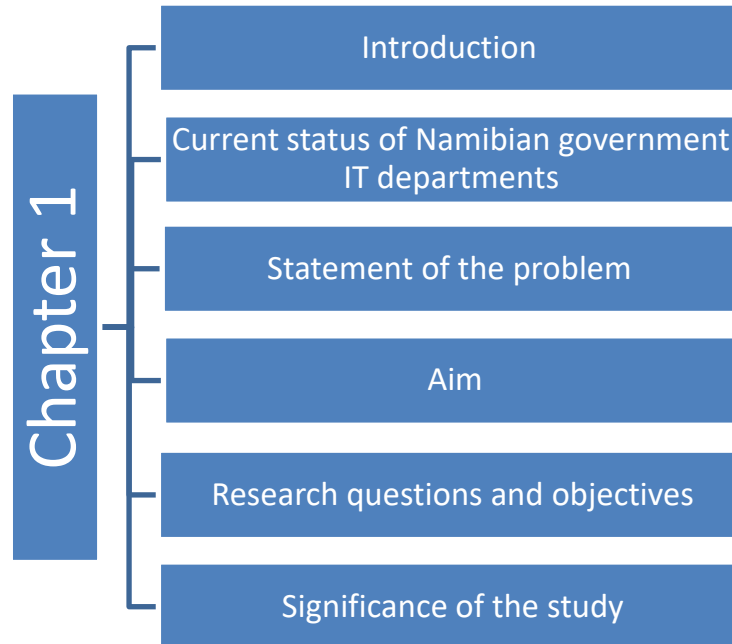
## **ABBREVIATIONS/ACRONYMS**

API	Application Programming Interface
AMI	Advanced Metering Infrastructure
ARP	Address Resolution Protocol
AWS	Amazon Web Services
CIA	Confidentiality, Integrity Availability
CPU	Central Processing Unit
CSP	Cloud Service Provider
DF	Decentralized Function
DoS	Denial of Service
DDOS	Distributed Denial of Service
DNS	Domain Name System
DSR	Design Science Research
EC2	Elastic Compute Cloud
HHS	Health and Human Services
IaaS	Infrastructure as a Service
ICT	Information Communication Technology
IP	Internet Protocol address
IS	Information System
IT	Information Technology
MAC	Media Access Control
MURD	Ministry of Urban and Rural Development
OMAs	Offices/Ministries/Agencies
OPM	Office of the Prime Minister
PaaS	Platform as a Service
PDCA	Plan Do Check Act
PS	Permanent Secretary
RC	Regional Council
ROI	Return on Investment
RTT	Round Trip Time
SaaS	Software as a Service
SCAF	Secure Cloud Adoption Framework
SLA	Service Level Agreement
SOAP	

SSH	Secure Shell Host
SSL	Secure Sockets Layer
TAM	Technology Adoption Model
TCP/IP	Transmission Control Protocol/Internet
Protocol	
TOE	Technological, Organisational and
Environmental	
WACS	West Africa Cable System

# CHAPTER 1: INTRODUCTION

Chapter 1 introduces the thesis as outlined:



## 1.1 Background

The ultimate objective of Namibia's Vision 2030 "is to improve the quality of life of her people to the level of other counterparts in the developed world" (Vision 2030, 2004). The Vision spells out national development programmes and strategies aimed at achieving the national objectives and provide a unified direction to both government and private sectors. One of the key focus areas is knowledge-based economy and information technology (IT). Nowadays, information technology is the driving force behind development and the Namibian government might be driven and prompted to consider solutions that reduce budget costs, such as cloud computing, to deliver efficient and effective information communication technology (ICT) services to its people (Nghihalwa & Bhunu Shava, 2018).

"The current information technology environment in the Namibian government is characterised by physical server infrastructure and wired network models, which are costly to maintain and sometimes the assets are underutilised. The Ministry of Urban and

Rural Development (MURD) has physical servers and a variety of other network equipment deployed at the 14 regional councils (RCs) in Namibia. This infrastructure requires high maintenance, regular inspection and hardware failure preventative measures, which are costly, and staff from MURD is required to travel from Windhoek to the regions to solve these issues” (Nghihalwa & Bhunu Shava, 2018). Physical servers in contrast to cloud-based servers are the traditional way of doing things in IT, which entails configuring hardware to meet the organisation’s needs (emails, Internet and other roles) (Mell & Grance, 2009).

Cloud computing is a new approach that reduces IT complexity by leveraging the efficient pooling of on-demand, self-managed virtual infrastructure, consumed as a service (Kuyoro, Ibikunle & Awodele, 2011, Nghihalwa & Bhunu Shava, 2018). According to Mell and Grance (2009), cloud computing is defined as 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) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Grispos, Glisson and Storer (2013) indicate that this phenomenon is increasingly becoming pervasive in today’s integrated networks and allowing institutions to reduce costs, and to develop more reliable and scalable computing solutions.

Cloud technology has three main service delivery models namely: Software as a Service (SaaS), Platform as a Service (PaaS) and IaaS. These services can be hosted on private, community, public or hybrid deployment models (Dawou et al., 2009). These models are accessible via the Internet and are made available when the user pays for the resources they need (Wyld, 2010). Researchers such as Wyld (2010), Grispos et al. (2013), Mell and Grance (2009), and Islam et al. (2013) concur and define these terms as follows: SaaS refers to the ability of the client to use the provider’s applications hosted on the cloud infrastructure. The applications are accessible from different client devices, for example, web-based emails. PaaS enables the client to deploy his applications onto the cloud using programming languages and tools supported by the cloud provider. The IaaS delivery model enables the client user to use the cloud infrastructure such as storage, networks, processing and other computing resources where the client can deploy operating systems and application. With IaaS, the client user does not manage the cloud infrastructure but has control over some selected network modules such as firewalls. Private cloud of the deployment models implies that the cloud infrastructure is dedicated

to a specific organisation. Several organisations share the cloud infrastructure for community cloud. Public cloud is cloud infrastructure that made available to the public. Lastly, hybrid cloud provides a composition of two or more clouds that remain a unique identity and assured by technology that enables data and application portability. **“This study focuses more on IaaS and SaaS, because PaaS provides a combination of infrastructure and applications, focusing more on software development processes, which hardly happen in government departments” (Nghihalwa & Bhunu Shava, 2018).** Considering the current needs, the Namibian IT departments focus more on getting the current setup working with limited costs and minimum service interruptions (Nghihalwa & Bhunu Shava, 2018). Hence, IaaS offers the government the infrastructure while SaaS caters for the applications needed for the crucial operational functions in the IT departments (Nghihalwa & Bhunu Shava, 2018).

This advanced cloud computing technology has the potential to improve government service delivery and reduce operating costs, and increase data centre efficiency and utilisation (Kundra, 2010). The cloud also offers advantages such as scalability, resilience, flexibility, efficiency and outsourcing (Kuyoro et al., 2011). However, with numerous technologies, such as “networks, databases, operating systems, virtualisation, resource scheduling, transaction management, load balancing, concurrency and memory management” accompanying the cloud, the paradigm faces security issues and challenges (Sen, 2013). Sen (2013) also argues that security in cloud is achievable through much assurance just like in traditional outsourcing. Unlike the traditional practice, there is no common cloud-computing standard. Each vendor implements own security technologies and standards. Sen (2013) further indicates how each of the IaaS and SaaS threats is a result of internal or external attackers.

Researchers such as Garfinkel and Shelat (2003) and Kundra (2010), caution that as technology evolves, organisations should ensure that standards are set for cloud computing platforms that provide security of the organisations’ information to protect the privacy of the citizens and safeguard national security interests. Wyld (2010) stresses that the cloud is shifting the way of doing things in IT for good irrespective of the uncertainties regarding security, interoperability and portability associated with it. It is inevitable that organisations and governments will adopt cloud-computing services, hence, there is a need to have security considerations upfront. This study seeks to analyse security issues and challenges in cloud-based services and propose a secure

cloud-based IaaS framework for the Namibian government IT departments. The framework will help Namibia prepare for cloud adoption with minimal security risks.

## **1.2 The status of IT departments in the Namibian government**

The Office of the Prime Minister (OPM) facilitates the process of formulation of policies and implementation of programmes of the Namibian IT department in government Offices, Ministries and Agencies (OMAs). OPM develops and maintains systems and investigates various OMAs' IT infrastructural needs and recommends specifications. MURD falls under OPM. The MURD IT department gives IT support to 14 RCs IT offices, which provide support services to the regional constituencies and the regional decentralised OMAs. According to Nghihalwa and Bhunu Shava (2018), the infrastructure of server rooms in IT departments is characterised by wired networks, servers, storage spaces and virtual machines. MURD IT personnel manage the servers and virtual machines. However, MURD faces challenges such as IT infrastructure, which is difficult and expensive to maintain, outsourcing of project expertise to private companies, few IT staff members, tedious hardware/software procurement process, and decentralised management and maintenance of IT infrastructure. Another challenge is the need for IT staff members to travel to regional centres to attend to major issues (Nghihalwa & Bhunu Shava, 2018).

## **1.3 Statement of the problem**

While traditional IT infrastructure faces low server utilisation, fragmented demand, is expensive to maintain and the systems are difficult to manage, cloud computing has the potential to improve government service delivery, reduce operating costs, increase data centre efficiency and server utilisation. Currently, the Namibian government is facing challenges of support personnel, who have to travel long distance from Windhoek to support branches in regions countrywide, IT infrastructure that is difficult and expensive to maintain, outsourcing of expertise and a tedious procurement process to purchase software or hardware. The study investigates the benefits and challenges associated with cloud-based infrastructure services, and propose a secure framework to adopt cloud computing in the Namibian government IT departments.

## 1.4 Aim

The aim of this study is to assess and investigate the benefits and challenges associated with adopting a cloud-based infrastructure service, readiness to adopt cloud computing and propose a framework for secure cloud adoption in the Namibian government IT departments.

## 1.5 Research questions and objectives

To achieve the study aim, the **objectives** of the study were:

- To analyse the cloud computing benefits for Namibia's government IT infrastructure and propose the best approach for adoption.
- To analyse security issues and challenges in adopting cloud based IaaS in Namibia's government institutions and propose secure solutions.
- To assess the Namibian government IT departments' readiness to adopt cloud computing.
- To propose a secure framework on how Namibian government can position itself to adopt to the cloud with minimum security risks.

To achieve the objectives, the following research **questions** were answered:

- What benefits does cloud computing yield to Namibian government's future IT infrastructure?
- What are the security issues and challenges in adopting cloud-based IaaS in Namibian government institutions?
- To what extent are Namibian government IT departments ready to adopt cloud computing?
- In what ways can the Namibian government position itself to adopt cloud-based computing services with minimum security risks?

## 1.6 Significance of the study

- Increased productivity and efficiency in the Namibian government's IT departments.



- The research will contribute to capacity building, as it can be used as reference material for migrating government traditional wired infrastructure to cloud infrastructure service.
- The outcomes would also contribute to the knowledge-based literature on the adoption of cloud computing services in the Namibian government IT departments and security risks involved.
- The research findings would assist directors and deputy directors in the Namibian government IT departments with decision-making and directives on whether to consider adopting cloud for the effective use of technology.
- The research results of adopting cloud services in Namibia would assist provide future guidelines on how to improve service delivery in the Namibian government IT departments.

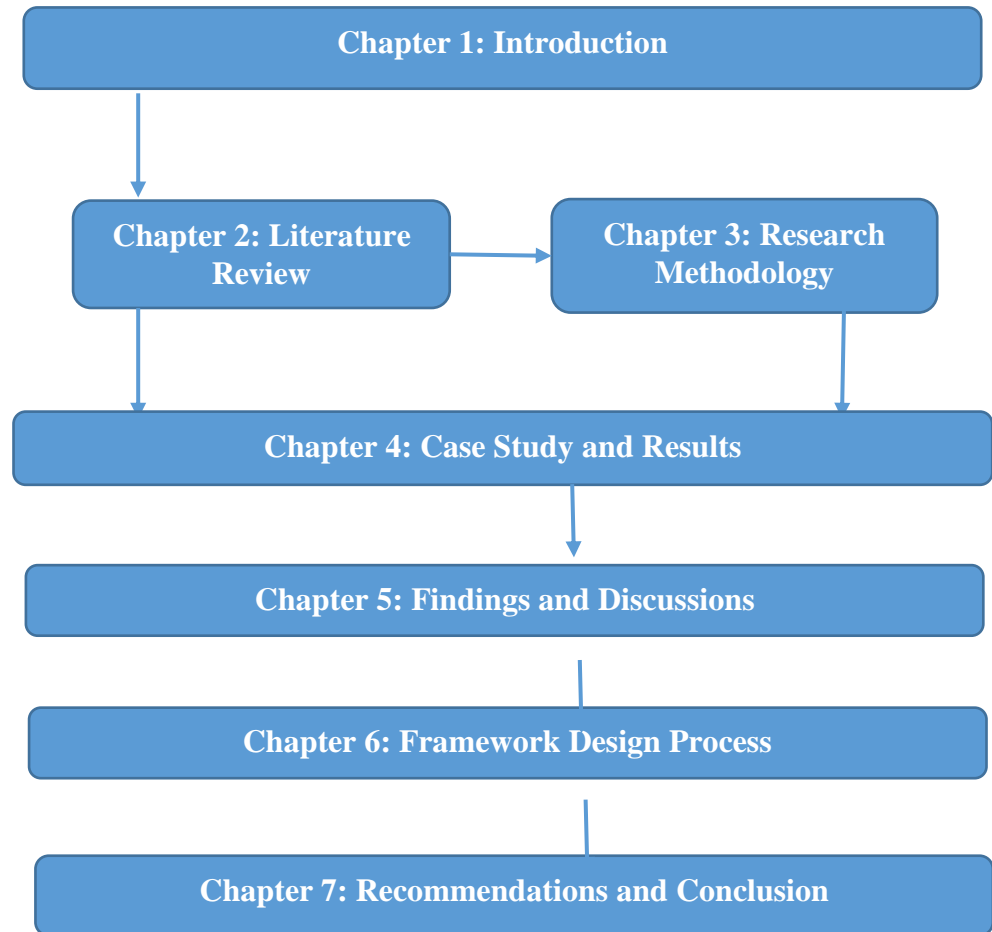
### **1.7 Limitations**

According to Bryman (2012), research is a process normally associated with challenges and these challenges define and limit the researcher from accomplishing the said objectives. The main challenge of this study was time constraint. It was difficult to assess all the Namibian government IT departments in all the ministries in the given research timeframe. As a result, the confinement to MURD IT department only might not give an accurate and representative conclusion of the investigated phenomenon in the Namibian context.

### **1.8 Chapter outline**

This thesis presents seven chapters. Chapter 1 introduces the whole thesis; it outlines the background to the research, the problem statement, objectives, research questions and the significance of the research. Chapter 2 discusses the literature review of the study. Chapter 3 discusses the research methods used to answer the research questions and achieve the study objectives. Chapter 4 presents the case studies conducted at OPM and MURD, including RCs and decentralised functions (DF), as well as the case study results. Chapter 5 presents the case study findings and discussions. Chapter 6 presents the framework design process and the proposed framework.

Chapter 7 concludes with reflections, lessons learnt, limitations, recommendations and areas of possible future research. Figure 1-1 is a pictorial representation of the research outline.

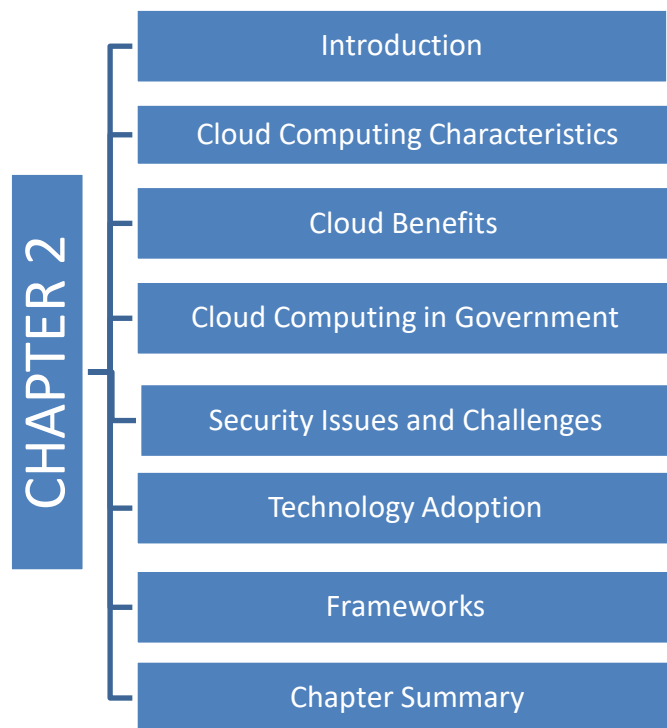


**Figure 1-1: Research outline**

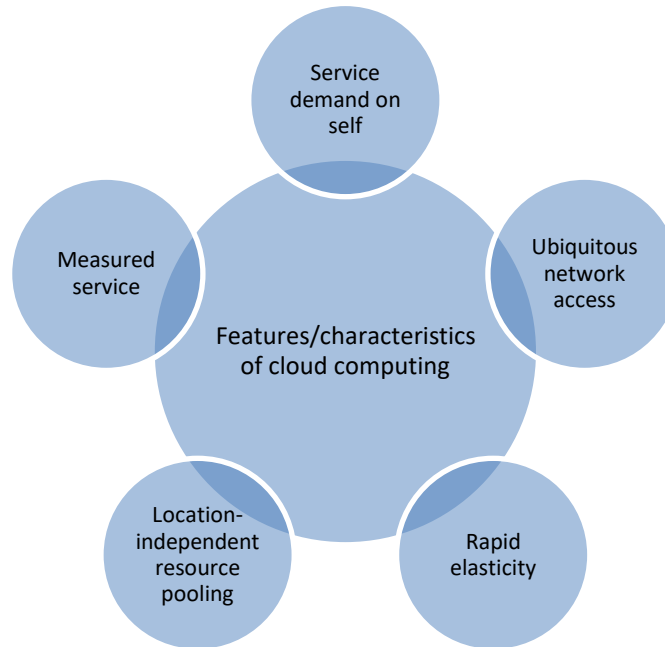
## CHAPTER 2: LITERATURE REVIEW

### 2.1 Introduction

This chapter reviews literature relevant to this study. The chapter gives an overview of cloud computing, cloud computing characteristics and discusses cloud computing benefits, security issues and challenges. It also discusses the case studies of cloud computing implementation in other countries' government departments. The chapter further discusses the technology adoption overview and frameworks. It concludes by presenting a chapter summary.



## 2.2 Cloud Computing Characteristics



**Figure 2-1: Characteristics of cloud computing**

NIST et al. (2011) and Hashemi, Monfaredi and Masdari (2013) list five essential characteristics of cloud as follows:

- **On-demand self-service:** This feature implies that customers can easily and automatically access services, such as server time and network storage, as needed, from the service provider.
- **Broad/ubiquitous network access:** This implies that the resources or facilities are widely available over the Internet and accessed through standard mechanisms such as mobile phones, laptops, and personal digital assistants.
- **Location-independent resource pooling:** This implies that the provider's computing resources (including storage, memory, bandwidth and virtual machines) are dynamically pooled to serve multiple consumers using a multi-tenant model.

- **Rapid elasticity:** With this feature, capabilities can be provided rapidly and flexibly, and customers can add, expand or release services quickly. The capabilities available are unlimited.
- **Measured service:** This cloud system feature enables automatic resource usage control, monitoring and reporting. Thus, providing transparency for both the provider and consumer.

This study found these cloud computing characteristics central in both government and private sectors.

## 2.3 Cloud Computing Benefits

According to Kundra (2011), the use of cloud service in government institutions promotes efficiency, agility and innovation through the effective use of IT investments. Kundra (2010) also compares the cloud benefits to the current IT environment and concludes that cloud innovation is efficient due to its resource utilisation and improved productivity (application development and management, network, and end-user) while traditional IT infrastructure faces low server utilisation, fragmented demand and the systems are normally difficult to manage. The study further reveals that cloud innovation is agile because it is available in the following formats: firstly, it can be purchased as a service, secondly, it is more flexible, as one can add or reduce its capacity and is more responsive to urgent calls. Meanwhile, it takes time to build new data centres for additional services and it is a lengthy process to increase capacity. Lastly, cloud is an innovative technology platform given that it shifts mindsets from asset ownership to service management, and supports entrepreneurship and emerging technologies. With current servers, most services are not compatible with new private innovation engines and require asset management at times.

Various researchers identified the following benefits of cloud technologies in contrast to the traditional IT infrastructure:

### a) Rapid Elasticity

According to Rajkumar, James and Andrzej (2011), the technology is designed to provide exceptional services with unlimited scalability. Resources can be purchased in any quantity at any time (Hashemi et al., 2013). The model's clients have access to a pool of

virtual resources, which allows them to respond to peak load with efficient, flexible and cost-effective techniques (Borko & Armando, 2010).

#### **b) Protection, Care and Technical Support**

Cloud providers are the hosts of the infrastructure and the applications as mentioned earlier. They are responsible for updating software and provide overall technical support, especially in remote areas. This reduces the workload for IT personnel and there is no need to travel long distances to solve problems in remote areas (Wojciech & Sergiusz, 2009). Hashemi et al. (2013) add that customers no longer need to update software applications on single computers, as a result it saves cost and time and there is less need for trained IT staff, especially in developing countries.

#### **c) Cost and Efficiency**

One of the main focuses of cloud is to provide affordable services to private organisations and the government sector. Eric and Bob (2010) highlight that the technology provides an opportunity for companies to shift from investment costing to operating costing by reducing the cost of expensive infrastructural systems such as servers and recruitment of IT experts to manage and maintain them.

#### **d) Auditing and Logging**

Tracing of any government information change is very crucial in e-government to avoid data manipulation in government agencies. Thus, with the aid of cloud, the process of controlling corruption in government becomes much easier, as security audits are frequently done by cloud providers to detect any fraud (Tripathi & Parihar, 2011). Cloud provides mechanisms that are available and reliable.

#### **e) Disaster Recovery**

According to Hashemi et al. (2013), it is very crucial for every organisation to have a disaster recovery plan in place in the event of any disaster. Cloud computing provides more disaster options to restore information quickly and efficiently than traditional disaster recovery (Rajkumar et al., 2011). Hashemi et al. (2013) further emphasize that governments can back up their servers daily and can also store it off-site using a third-party storage service provider.

#### **f) Reporting and Intelligently**

To maximise resource utilisation, cloud computing monitors and reports events such as storage, network and central processing unit (CPU) of data centre and the consumption level to distribute the peak load effectively (Tripathi & Parihar, 2011). Tripathi and Parihar (2011) further indicate the capability of cloud to profile data, making it visible to every citizen.

#### **g) Policy Management**

It is very important for every country to ensure that policies and regulations are implemented. Cloud provides for these policies to be implemented in the data centre for the effective use of data and improved performance. Hashemi et al. (2013) narrate that it is very crucial for security policies to be deployed also at applications in the data centres.

#### **h) Systems Integration and Software Legacy**

Tripathi and Parihar (2011) emphasise that cloud provides integrated cloud-based applications, offering best solutions for various systems to be integrated and transferred to cloud. This enhances data correlation across applications, providing fast services to citizens.

#### **i) Old Technologies and Migrating to New Technologies**

With the current practice of e-government, it is always a challenge to transition from old technology to new technology. With the proposed e-government policies, cloud can integrate e-government applications. The cloud technology provides the ability to run different versions of applications concurrently (Mahafuz & Sakibur, 2011).

#### **j) Green Technology**

According to Hashemi et al. (2013), use of ICT systems in the government sector has had a negative impact on the ecosystem that has seen an increase in the rate of carbon dioxide production and increased power consumption. Power consumption and e-waste in the air can cause environmental hazards. The cloud paradigm, through virtual services, protects the eco-systems and power consumption is reduced.

Considering the above-mentioned benefits, government institutions are more fascinated with the possibility of using the cloud computing services mainly to reduce IT costs, increase capabilities and expand their service delivery (Morsy, Grundy & Müller, 2010). Although cloud computing represents the new computing model (Dawou et al., 2009), organisations are still sceptical about its authenticity.

Based on a survey conducted by IDC (2008), the adoption of cloud computing is associated with challenges and security issues, as discussed later in this paper. Kundra (2011) suggests that the risk assessment team should consider both security benefits and vulnerabilities in cloud computing. Regardless of the challenges noted, Kundra (2011) highlights the potential security benefits, which include the ability to focus resources on areas of high concern, great uniformity and homogeneity, which promote data assurance, security response, system management, reliability and maintainability. Due to services on demand, the availability of resources is improved through scalability, redundancy, disaster recovery, resilience, improved backup and recovery capabilities, policies, procedures and consistency (Kundra, 2010; 2011).

However, the cloud security for IaaS and SaaS remains an issue of concern. Confidentiality, integrity, availability, authenticity and privacy are concerns for both cloud providers and government agencies.

## **2.4 Cloud Computing in Government**

Across the globe, governments are looking for the best technological ways to perform daily activities that improve interactions with citizens through providing efficient and effective services (Nghihalwa & Bhunu Shava, 2018). The use of the latest technologies fast-tracks processing time needed to deliver service to citizen. Hashemi et al. (2013) describe the process of using ICT to “improve efficiency and effectiveness, transparency and comparability of financial and information exchanges within the government, between the government and citizens, and between government and private sector” as e-government. Many countries, including Namibia, have attempted to implement e-government to improve government service delivery, empower citizens through increased access to information and increase the ability to interact and collaborate, and transparency and accountability as well as improve the relationship between the



government and citizens through electronic delivery (Gopala, Vishnu & Madhusudhana, 2009).

E-government provides the government with an integrated solution with cloud technology (Kuldeep, Shravan & Amit, 2012). Cloud increases collaboration among different organisations within the government, it reduces data redundancy and promotes the effectiveness of government through tracking and monitoring their plans (Hashemi et al., 2013). Thus, the cloud paradigm also assists in reducing repetitive operations and maximises the use of government resources.

According to Tripathi and Parihar (2011), e-government faces effective challenges that are linked to social, economic and political barriers, which “limit the scope of policymakers’ activity for effective use of new technologies” (Hashemi et al., 2013). Data scaling, system integration, legacy software, disaster recovery, auditing, obsolete technologies and policy management are some of the technical challenges e-government faces (KPMG, 2011). However, cloud computing provides solutions to these challenges.

West (2010) reviewed past studies and analysed case studies of government institutions that moved to cloud services and based on the analysis, he recommends five steps that improve efficiency and operations in the government sector:

1. The government needs to redirect more resources to cloud computing to reap efficiencies represented by that approach,
2. The General Services Administration should compile data on cloud computing applications, information storage, and cost savings to determine possible economies of scale generated by cloud computing,
3. Officials should clarify procurement rules to facilitate purchasing through measured or subscription cloud services and cloud solutions appropriate for low, medium, and high-risk applications,
4. Countries need to harmonise their laws on cloud computing to avoid a “Tower of Babel” and reduce current inconsistencies regarding privacy, data storage, security processes, and personnel training, and
5. Lawmakers need to examine rules relating to the privacy and security of cloud computing to ensure safeguarding of information in the system.

Wyld (2010), a researcher on cloud computing and the public sector around the world, also talks about universal connectivity, open access, reliability, interoperability and user choice, security, privacy, economic value and sustainability as essential for the cloud model to work successfully in government. Wyld (2010) advises learning, organisational assessment, cloud pilot, cloud readiness assessment, cloud rollout strategy and continuous cloud improvement, as the six steps to migration strategy in government.

### **2.4.1 Case Studies of Cloud Computing Adoption in Government**

Study has found that cloud computing is increasingly being implemented across public sectors worldwide with government leading in the deployment of cloud computing (Wyld, 2010). Wyld (2009, 2010) examines non-military uses of cloud computing in government, from the United States to Europe and Asia and the following section presents a summary of case studies of cloud adoption in government in those regions. In Africa, Xi and Mitrovic (2014) conducted similar studies on readiness to adopt cloud computing in Western Cape Provincial Government, South Africa.

#### **2.4.1.1 South Africa**

The South African study focused on assessing cloud computing reading based on three indicators namely: infrastructural, organisational and environmental. Their findings revealed concerns over electricity supplies, the absences of a communication strategy to advocate for cloud computing adoption and security concerns. Despite these concerns, Xi and Mitrovic (2014) assert that respondents viewed cloud computing as a green economy initiative because of its energy and cost saving aspects. In addition, the concerns were likely to be offset by the commitment of the Provincial Government of Western Cape.

#### **2.4.1.2 United States Government**

In the United States, the government has explored cloud computing adoption to deliver services as detailed below:

The General Services Administration aims to provide IaaS for all government agencies, through a certified (security, privacy and capabilities) vendor (Hoover, 2009). Amazon and eBay storefronts allow the agencies to mirror from the private sector and acquire the best cloud solution. Apps.gov was the perfect solution and an improvement on government data management and completion of tasks (Weigelt, 2009).

In 2009, the National Business Center, a service provider for federal agencies in the Department of Interior, was seeking to be a cloud provider. It operated cloud-based human resource management applications, including web-based training, staffing and recruitment programmes. It was also slowly offering cloud-based financial and procurement software (NBC's Federal Cloud, 2009).

In the same year, the Department of Health and Human Services (HHS) Program Support Center was running a working online SaaS pilot to provide over 60 services to HHS and other government agencies (Gross, 2009). Hence, this provision can be applied to the Namibian government to provide services to the citizens.

The US Census Bureau employed Salesforce.com's SaaS to manage the activities of about 100,000 partner organisations, however, the agency decided to store its census data on its own internal servers because of security and privacy concerns with the cloud (Hart, 2009). Hart (2009) further reveals that for the organisation to give its data, it needed to trust cloud providers. The study emphasises trust between cloud providers and cloud users when SaaS and IaaS is implemented.

The White House is using Google Moderator to help determine which questions should be asked from the public and allow for public voting (Arrington, 2009). Cloud-based application allowed for hundreds of thousands of votes to be cast on the almost 10,000 questions that were submitted for possible use in the live event with the president (Wyld, 2010). Furthermore, the Office of Management and Budget looked to cloud computing as a way through which state and local agencies, who receive stimulus funds, reported on

the use of the monies and allowing citizens to track the results online. This indicates that cloud computing is the future in bringing government service delivery closer to the citizens.

#### **2.4.1.3 European Government**

The United Kingdom's strategy priority is the G-Cloud, the government's wide cloud computing network (Glick, 2009). The strategy is to improve the governmental IT industry and allows more services to be migrated online. It believes in delivering public services at large and as the owner of data systems. The public sector has influence in many areas such as education, health and defence, hence, the need to deliver up to standard services (Digital Britain, 2009).

According to Petrov (2009), European nations are exploring the use of cloud computing in these areas: management of public sector housing, transportation service networks, economic development, census, health services, contracting and education services.

#### **2.4.1.4 Asian Government**

Japan's national government took the "Kasumigaseki Cloud" cloud computing initiative. The initiative is named after a section in Tokyo where Japanese ministerial offices are located (Hicks, 2009). The Kasumigaseki Cloud sought to develop a private cloud environment that would accommodate all the Japanese government's computing to "allow for greater information and resource sharing and promote more standardisation and consolidation in the government's IT resources". The Japanese government believed that combining all governmental IT functions under a single cloud would not only reduce costs and operations, but also promoted a friendly IT operations environment (Rosenberg, 2009).

In Dongying, a cloud initiative headed by local leaders called The Yellow River Delta Cloud aimed at improving e-government offerings and economic development was established and the same applied to the city of Wuxi, where the municipalities set up a cloud services factory to improve the computing resources available to local companies. The initiative was prompted when Wuxi did not have enough finance to build proper traditional IT infrastructure (IBM, 2009).

The Government Information Technology Service established a private cloud used by Thai government agencies. They already have a cloud-based e-mail service and were planning to add SaaS (Hicks, 2009).

The Ministry of Commerce in Singapore combined all government agencies IT procurement, focusing on IT acquisition and investigating how cloud computing and SaaS were of importance to them (Strecker, 2009).

For the above-mentioned case studies, Weigelt (2009) mentioned that there are eight fundamentals that are important in enabling the cloud computing concept. It is essential that cloud computing models should be or include universal connectivity, open-access, reliability, interoperability and user choice, security, privacy, economic value and sustainability. The cloud migration strategy involves a six-step process (Weigelt, 2009). Firstly, the cloud migration strategy begins with learning about the basics of cloud computing - through attending seminars, networking, talking with vendors, and reading. Secondly, organisational assessment. IT managers should conduct an assessment of their present IT needs, structure and capacity utilisation. In a cloud computing environment, where resources can be added or subtracted based on needs and demand, it will be critical for IT managers to honestly assess their IT baseline. Thirdly, IT managers should do cloud piloting and assess their ability to manage and bring such a project to fruition. Fourthly, cloud-readiness assessment. IT managers should then conduct an overall IT cloud-readiness assessment to determine if their organisation has data and applications that could readily move to a cloud environment, and if a public/private/hybrid cloud would be suitable or usable for these purposes and rank-order potential projects. As this assessment progresses, IT decision makers must focus on establishing decision rules as to which data and applications can and cannot be housed in any form of cloud environment. The fifth step involves cloud strategy roll out. The last step involves continuous cloud improvement. The organisation continues to move data to the cloud and do continuous assessment of cloud technologies and put all policies and strategies in place.

The IaaS and SaaS have the potential to become the government's sourcing strategy, however, the challenge remains with security. Many governments' agencies that have implemented the cloud are still hesitant about this, but slowly and surely models and solutions are being developed to close this gap. As Namibia emerges to fulfil her Vision

2030 of becoming a developed country, solutions of this kind (cloud computing) are of interest. Hence, the need to investigate and assess the adoption of cloud IaaS in the Namibia's government IT departments and propose a secure framework for adopting cloud computing services in Namibia with minimal security risks.

## **2.5 Cloud Computing Security Issues and Challenges**

Researchers have shown great evolving adoption of cloud both in private and public organisations across the globe, especially in United States, Europe and Asia. Less effort has been made in African government agencies, such as Namibia. However, maintaining security using the new advanced technology remains a challenge for both private organisations and the government sector. Security is the biggest obstacle in some private and government institutions accepting cloud advances (Kuyoro et al., 2011). Cloud security not only impacts what is on the cloud but puts the entire company at risk. Many are wary of trusting someone else with their organisation's data and deploying their software or applications on storage they have no control over. Researchers (Hamlen et al., 2010; Morsy et al., 2010; Kuyoro et al., 2011; Sen, 2012; Dawou et al., 2008) investigated the general security risks associated with cloud delivery models depending on data sensitivity, cloud architecture and security controls.

According to Sen (2013), there are information security vulnerabilities that are a concern to every organisation's confidentiality, integrity and availability (CIA) of data:

### **2.5.1 Confidentiality**

Outsourcing of an organisation's data simply means losing control over it. The threat of insiders and external attackers and third-party consultants accessing customers' data held within the cloud can be frightening. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property will be subjected to attacks by groups with significant resources that will be attempting to retrieve data. This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.

A threat from widespread data leakage among many, potentially competitor organisations using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise.

Ertaul, Singhal and Saldamli (2010) suggest that customers have anonymous access to their data, using HMAC-SHA1 signature to authenticate their access using the user's private key.

### **2.5.2 Integrity**

Integrity is an important aspect of any organisation. It ensures that the right and authorised people have access to the right information. For configurations within a complex service delivery such as SaaS, sharing computing resources could present a threat against data integrity in case of poor identity and access management procedures. Implementation of poor access control procedures creates many threat opportunities, for example, if disgruntled ex-employees of cloud provider organisations maintain remote access to administer customer cloud services, they can cause intentional damage to their data sources.

Threat or impact on data quality increases as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing the infrastructure.

### **2.5.3 Availability**

As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services.

The threat of denial of service against available cloud computing resources is generally an external threat against public cloud services. However, the threat can impact all cloud service models, as external and internal threat agents could introduce application or hardware. Denial of service (DoS) is caused by threats such as network bandwidth

distributed network domain name system (DNS), application and data denial of service components.

The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data centre facilities and have considered resilience among other availability strategies.

There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice. The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in-house systems in parallel with those managed by third-party cloud service providers. If these procedures are not tested, then the impact upon recovery time may be significant.

#### **2.5.4 Network security attackers**

Ertaul et al. (2010), in a research on the network security measures associated with the cloud technology, list and explain the following:

**-Distributed Denial of Service (DDOS) Attack:** In this case, the attackers send a large amount of network traffic and users are denied access to services. “In order to stop hackers from attacking the network, subscriber or provider faces blackmail” Ertaul et al. (2010). Amazon provides networks that are multi-homed across providers to promote diverse Internet access (Amazon, 2009).

**-Man in the Middle Attack:** This attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when, in fact, the entire conversation is controlled by the attacker (Williams, 2006). All the Amazon Web Services (AWS) Application Programming Interface (APIs) are available via Secure Sockets Layer (SSL)-protected endpoints, which provide server authentication. Amazon Elastic Compute Cloud (EC2) Advanced Metering Infrastructure



(AMIs) automatically generate new Secure Shell host (SSH) certificates on first boot and logs them to the instance's console (Amazon, 2009).

- **Internet Protocol (IP) Spoofing:** Spoofing is the creation of TCP/IP packets using somebody else's IP address. Intruders gain unauthorised access to the computer, whereby he sends messages to a computer with an IP address indicating that the message is coming from a trusted host (Williams, 2006). Mechanisms such as host-based firewall infrastructure provided by Amazon will not allow traffic being sent with a source IP or MAC address other than its own (Amazon, 2009).

- **Port Scanning:** If the subscriber configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. Since a port is a place where information goes into and out of the computer, port scanning identifies open doors to a computer (Williams, 2006). Williams (2006) further adds that cloud computing uses cloud middleware software to follow protocols to prevent port scanning, hence protecting cloud technologies from port scanning scams.

- **Packet Sniffing:** Packet sniffing is when other tenants are listening (with software) to the raw network device for packets that interest you. When that software sees a packet that fits certain criteria, it logs it to a file (Williams, 2006). Cloud does not allow sniffing/access to other tenants' data, as it uses a malicious-sniffing-detection platform that is based on Address Resolution Protocol (ARP) and Round Trip Time (RTT) that is basically used to detect a sniffing-system that is running on a network says Williams (2006).

### 2.5.5 Security

Several researchers point at security issues in virtual environments as the biggest challenge to cloud adoption. Ertaul et al. (2010) illustrate that in virtualised platforms, security issues are more difficult, as cloud providers have to maintain security both on physical and virtual hosts. The risks come in when the security on the physical host is compromised, then most of the virtual instances residing on that server are affected.

It is advisable that providers separate cloud instances (of different customers) running on the same physical machines. Steve (2009) argues that although security in a traditional data centre still applies in cloud, “physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server” (Ertaul et al., 2010).

Steve (2009) adds that the technology offers administrative (built-in, configured and management protection) host operating systems to business administrators. Access is, therefore, logged and audited. In case the business no longer exists, the privileges and access to those hosts are revoked.

Morsy et al. (2010) analysed the cloud computing security problems and summarise them as follows: some security problems are inherited from the used technologies, multi-tenancy and isolation, security management is very critical to control and manage, and the cloud should have a holistic security wrapper. Morsy et al. (2010) recommend these solutions based on the security problems discussed: problem abstraction using approaches to capture different security views, inherent in the cloud architecture, support for multi-tenancy, integration and coordination with other security controls at various layers to deliver integrated security and being adaptive to meet continuous environment changes and stakeholders. Kuyoro et al. (2011) highlight the key security considerations and challenges that are faced in cloud computing such as security, costing model, charging model, service level agreement, what to migrate and cloud interoperability issues. Hamlen et al. (2010) also discussed storage security, data security, network security and secure virtualisation as issues for cloud computing and believe that building trusted applications from untrusted components will be a major aspect in securing cloud computing.

A study by Dawoud et al. (2009) to investigate IaaS security components identifies challenges that are associated with IaaS implementation and deployment as service-level agreement, utility computing, cloud software, platform virtualisation and networks and Internet connectivity. Dawoud et al. (2009) propose an IaaS security model as a guide for assessing and enhancing security in each layer of the IaaS delivery model.

#### **2.5.6 Cloud security solutions**

Table 2-1 presents the security solutions of the issues identified:

**Table 2-1: Cloud Security Solutions**

Security and Privacy requirement	Solutions	Authors
Authentication	Username, passwords, use additional authentication factor (2FA)	Youssef and Alageel (2012) Ertaul et al. (2010) Williams (2006)
Authorisation and access control	-Restrict cloud admins' hiring process -Monitor activities of authorised users -Build trust between cloud service providers, cloud customers and admins	
Confidentiality	-Employ strong authentication methods -Prevent unauthorised access -Use encryption techniques	
Integrity	-Use encryption and hash algorithms -Prevent unauthorised access	
Non-repudiation	-Digital signature -Timestamps -Confirmation receipt services	
Availability	-Use backup and recovery schemes	
Compliance and audit	-Perform internal and external audits on a regular basis to monitor cloud service provider's compliance to agreed terms, standards and regulations	
Transparency	-Provide customers with clear information on controls, security and operation of the cloud -Refer to Service Level Agreement	
Governance and accountability	-Effective implementation and adherence of security policies and procedures to protect clouds from threats and data loss	
Attacks and Threats	Solutions	Authors
Denial of Service (DoS)	-Provide more computational power and resources	
Wrapping attacks	-increase security during message passing from the webserver to the web browser by using the SOAP message	
Cloud injection attacks	-Use hash algorithms	

Metadata spoofing attacks	-Use verification tools	Youssef and Alageel (2012)  Ertaul et al. (2010)  Williams (2006)
Malicious insiders	-Require transparency in all information security issues -Define security breach notification process -Enforce strict hiring requirements and human resource assessment	
Shared technology	-Conduct vulnerability scanning and remediation -Promote strong authentication and monitor unauthorised activities -Implement security best practice for installation and configuration	
Data loss or leakage	-Implement strong application programming interface (API) control, key generation and encryption techniques -Provide backup and retention strategies -Analyse data protection at both design and run time	
Lack of governance	Carefully execute SLAs	
Lack of compliance	Perform regular audits for compliance	
<b>Risks</b>	<b>Solutions</b>	<b>Authors</b>
Trust: Data location	-Provide consumers with information on where their data is stored and processed	Youssef and Alageel (2012)  Ertaul et al. (2010)  Williams (2006)
Data recovery	-Backup data at other data centres	
Data Segregation	-Use encryption and distributed storage to prevent data seize	
Data remanence	-Ensure the deletion of data after use of cloud service	

## 2.6 Technology adoption overview

According to Sharma and Mishra (2013), technology adoption is one of the mature areas of research in information systems. Technology adoption is defined as the stage of selecting a technology for use by an individual or an organisation (Carr, 1999). Davis (1989) says the Technology Adoption Model (TAM) has been widely used in technology adoption studies such as cloud computing. Davis (1989) further narrates that the model has two strength factors, namely perceived usefulness and perceived ease of use. Perceived usefulness is defined as the degree to which a person believes that using a particular system would enhance his or her job performance. Perceived ease of use is

defined as the degree to which a person believes that using a particular system would be free of effort. The benefits and security issues and challenges previously discussed promote cloud computing adoption. The next section discusses the frameworks that aid cloud computing adoption.

## **2.7 Frameworks**

A framework is defined as an outline of interlinked ideas, which supports a particular approach to a specific objective, and provides a frame of reference that can be modified as and when required (Shackel, 2009; Zachman, 1987). Furthermore, von Roessing (2010) details that frameworks provide a comprehensive descriptive structure of how to implement, create or manage a program or process. According to Mpekoa (2013), the purpose of constructing a framework is both descriptive and critical. The framework assists in understanding and communicating identified problems and gaps in the current theory and yet enhancing the contribution of the researcher (Zachman, 1987).

The next section discusses the types of cloud computing adoption frameworks in existence.

### **2.7.1 Existing Frameworks in Cloud Computing Adoption**

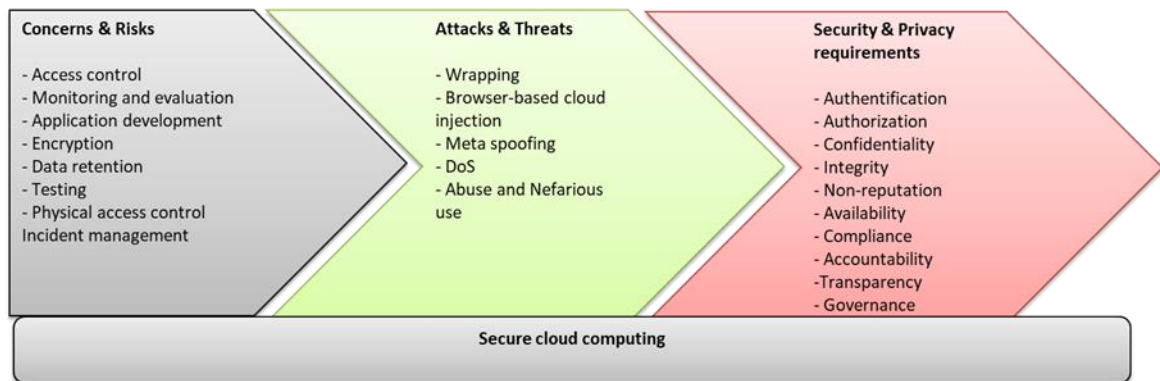
This section presents the frameworks developed by other authors' essentials for cloud computing adoption. According to Youssef and Alageel (2012), there are frameworks that can be implemented to help cloud computing adoption. This study discussed five frameworks.

#### **2.7.1.1 *A framework for secure cloud computing***

Youssef and Alageel (2012) propose a framework that identifies security and privacy challenges in cloud computing. It highlights cloud-specific attacks and risks and clearly illustrates their mitigations and countermeasures. Youssef and Alageel (2012) advise on the security and privacy solutions that should be considered when using the cloud environment.

Figure 2-2 shows the framework for secure cloud computing (Youssef & Alageel, 2012). It consists of three essential security components; each of them includes important challenges related to cloud security and privacy. These components are: “Security and privacy requirements: identify security and privacy requirements for cloud such as authentication, authorisation, integrity, etc. Attacks and threats: warn against different types of attacks and threats to which cloud is vulnerable. Concerns and risks: pay attention to risks and concerns about cloud computing” (Youssef & Alageel, 2012).

This study adapted these essential security components that help mitigate the security and privacy issues, attacks, threats, concerns and risks associated with the deployment of cloud. Along with the framework, they proposed a generic cloud security model that helps satisfy security and privacy requirements in cloud and protect them against various vulnerabilities.



**Figure 2-2: A framework for secure cloud computing (Source: Youssef and Alageel, 2012)**

### **2.7.1.2 A security framework in cloud computing infrastructure**

Harfoushi et al. (2016) identify a Technological Organisational Environmental (TOE) framework developed by Tornatzky and Fleischer (1990) that specifies three components (TOE) that drives the organisations to embrace cloud computing. These TOE elements seem to be more valuable in employing technology adoption compared to others (Harfoushi et al., 2016). This study identified the framework comments according to these TOE framework components.

- Technological context: means the internal and external technologies that organisations can use in the business. Technologies that are currently used by the firm

influence the decision of adopting cloud computing because they determine the scope and limit of the technological change that the firm can accept. Awa et al. (2015) argue that the successful adoption of IT depends on the technological competence of the organisation.

- Organisational context: means the resources and characteristics of the organisations. Organisational context consists of two main components - top management and technological readiness. Top management support plays a significant role in initiating, implementing, and adopting of IT. Their support can be seen in their sponsoring of initiatives and engaging in the adoption of cloud computing within the organisation. Top management awareness of potential benefits of adopting cloud computing is regarded as essential to manage potential organisational change through pressed vision and commitment, sending positive vibes of confidence in the new technology to all employees. Technological readiness means the readiness of infrastructure and IT human resources, which influence the adoption of cloud computing.

- Environmental context: covers the environment where the organisation operates. This includes competitors, trade partners, government policy and vendor scarcity (Awa, 2015). Cloud adoption promotes a competitive environment by industry structure and outperforming other organisations and with overwhelming cloud benefits, the first organisations are expected to derive these benefits in terms of competitive advantages and survival (Gangwar, Date & Ramaswamy, 2015). Trading partners include cloud service providers. Organisations rely on the cloud services providers' experience, skills and the ability to deliver or to make services available when needed. Security and accountability of the service providers play an important role. Vendor scarcity refers to the lack of reputable and qualified cloud service vendors in the cloud service market in Namibia. The availability of enough vendors with good reputation improves the organisation's confidence in cloud services. According to Li, Zhao and Yu (2015), vendor scarcity has a negative influence on the organisation's trust in cloud computing.

This study embraced this TOE framework and used it as a starting point to analyse and categorise the identified components based on the TOE factors.

### **2.7.1.3 Security framework for governmental cloud**

The “security frameworks for governmental clouds”, developed by ENISA (2015) are modelled in phases, security activities and steps that detail the set of actions to be followed for the definition and implementation of secure governmental cloud.

Firstly, this framework detailed the roles of the involved parties and responsibilities each has on the implementation of the framework. According to ENISA (2015), these roles comprise:

- Cloud owner: Is the organisation that legally owns the cloud, defines policies and requirements.
  - **Example:** In the Namibian context, the Namibian government will legally own the cloud, through the OPM.
- Cloud service provider: Is the organisation that provides cloud services based on the SLA and makes these services available to the cloud customers.
  - **Example:** The Namibian government will have to choose a cloud service provider to provide IaaS and SaaS.
- Cloud customer: Is the organisation/public administration using the cloud services provided by cloud service providers through cloud owners.
  - **Example:** Government employees from OMAs and RCs will access the available cloud services of the government cloud through the OPM.

Secondly, the study (ENISA, 2015) identified the logic model phases following the Plan, do, check and act (PDCA) model cycle: plan, do, check and act to model information security management systems into the governmental clouds. The PDCA model is often adopted in information security because of its notion on evaluation (check), updates (act) and the identified steps, which are very crucial in all networks and information security aspects. This framework covers the security decision.



Table 2-2 presents an overview of the security framework for governmental clouds based on the PDCA lifecycle.

**Table 2-2: Plan-Do-Check-Act lifecycle**

Lifecycle Phase	Security Activities	Security Steps
<b><u>PLAN</u></b> This phase focuses on setting policies, and a strategy for implementing controls to achieve security objectives	Risk profiling	Identify services to cloudify
		Select relevant security dimensions
		Evaluate individual impact to dimensions
		Determine global risk
	Architectural model	Decide on the deployment service model
	Security and privacy requirements	Establish security requirements
<b><u>DO</u></b> This phase involves implementing and operating the controls, i.e, controls are executed in the DO phase	Security Controls	Selection of security controls
	Implementation, deployment and accreditation	Formalisation and implementation of the selected security controls
		Ex-ante verification of suitability of the cloud service to provide a sufficient level of assurance
		Start service execution
<b><u>CHECK</u></b> This phase is focused on the review and evaluation of the performance (efficiency and effectiveness) of the system. Tests are performed to ensure that controls are operating as intended and meet objectives	Log/monitoring	Periodically check that security controls are in place and being followed
	Audit	Verification that the defined/contracted levels of security are fulfilled

<b><u>ACT</u></b> This phase involves the remediation of deficiencies or gaps identified in the CHECK phase. Changes are made where necessary to bring the system back to the planned performance.	Changes management	Implementation of remedies and improvement to the security framework/approach
	Exit Management	Contract termination, return of data to customer and data deletion

#### ***2.7.1.4 Control framework for information and related technology***

Control Framework for Information and related Technology (COBIT), this is a “framework for IT governance and control. It supports toolsets that allows managers to bridge the gap between control requirements, technical issues and business risks” (ISACA, 2010). As a governance and control framework, COBIT provides two procedures - one for defining an IT strategy and the second for managing third-party services. It also provides a maturity model that can be used to assess the maturity of the IT governance processes in an organisation. For cloud computing clients, by using the COBIT procedure, the client will be able to determine what should be done before and after selecting a cloud solution. According to Shimba (2010), COBIT helps in monitoring the value that is to be gained by adopting cloud computing, the level of risk exposure and in deciding who will be responsible, accountable, consulted and informed during the cloud adoption project. The maturity model will help an organisation in determining the level of maturity of its IT governance, and whether the maturity level is acceptable for the move to cloud computing. Therefore, by using COBIT, an organisation can institutionalise good practices which will ensure that IT investments produce business value (ITGI, 2007). And in this case, it will help in ensuring that the move to cloud solutions will result in better business value without compromise.

#### **2.7.1.5 A decision framework for cloud computing**

A study by Kaisler, Money and Cohen (2012) developed a decision framework to help managers determine which cloud solutions match the specific requirements for their organisations. Kaisler, Money and Cohen (2012) further narrate that moving to cloud computing requires decisions in three categories, namely, service architecture, system architecture and application architecture. Service architecture assesses how the service is provided and the view of the user on the cloud computing. System architecture assesses the cloud infrastructure issues and the cloud-based applications. While application architecture assesses how applications are mapped to the cloud infrastructure.

This framework demonstrates that decision making is very important when adopting cloud computing.

### **2.8 Chapter Summary**

This chapter reviewed cloud computing technology and provided an overview of cloud computing definitions, characteristics, benefits, security and privacy issues and challenges.

The study reveals that cloud computing is beneficial to government institutions because of the following benefits: flexibility, elasticity/scalability, cost efficiency, provides audits, disaster recovery, improved backups, reports intelligently, policies management, service delivery and promotes data assurance. This study examined the extent to which these benefits affect the adoption of cloud computing services in the Namibian government IT departments.

This chapter also identified the security and privacy issues and challenges in cloud computing. An analysis of the security and privacy challenges, issues, attacks and risks concerns regarding data protection, compliance to policies and legal issues and solutions have been provided. This study focused on further exploring and analysing the best solutions to security issues and challenges that are best suited for the Namibian government IT departments.

It is also evident from this chapter that proposed secure and governance frameworks for cloud computing adoption do exist. This chapter analysed five frameworks that provide and contain important components needed for the design of the framework proposed in this study. Firstly, in “a framework for secure cloud computing”, the study adapted the security essential components that help to mitigate the security and privacy issues, attacks, threats, concerns and risks associated to the deployment of the clouds as presented in Figure 2-2. Secondly, Section 2.4.1.2 discussed “a security framework in cloud computing infrastructure”. This framework identified a TOE framework that specified three components TOE that drive the organisations to embrace cloud computing. These TOE components informed this study on the importance of grouping the identified sub-components based on the technological factors, organisational factors and environmental factors. Thirdly, this chapter considered “security framework for governmental cloud”, this framework entails the phases, security activities and steps that needed to be followed for the definition and implementation of a secure governmental cloud. The framework detailed the roles of each party involved and their responsibilities as demonstrated in Section 2.4.1.3. Furthermore, it identified logic model phases following the PDCA model cycle to model information security management systems into the governmental clouds. Fourthly, the chapter also discussed the proposed security and governance framework for cloud computing based on security standards and the COBIT best practices presented in Section 2.4.1.4. Lastly, the “A decision framework for cloud computing” demonstrated that decision making is very crucial in the implementation of cloud computing.

As observed above, all these frameworks lack a component that is an aid needed for the successful secure adoption and implementation of cloud computing. The chapter also highlighted the recommended five steps to improve efficiency and operations in government. This was very important in informing the theoretical framework of this study:

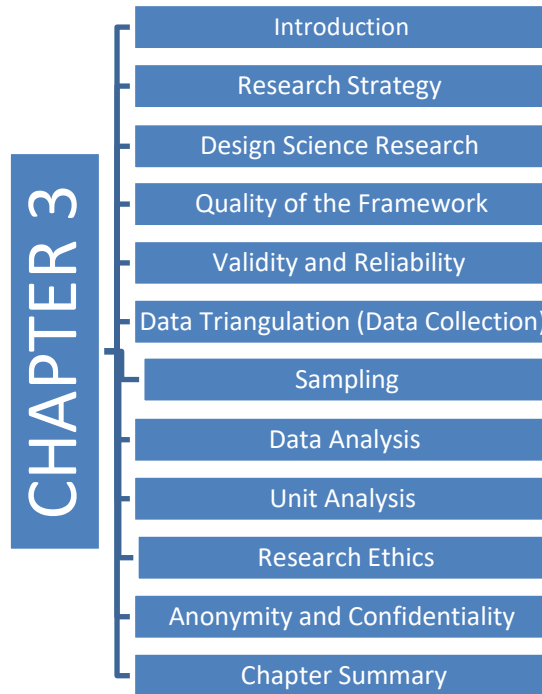
1. The government needs to redirect more resources to cloud computing to reap efficiencies represented by that approach,
2. The General Services Administration should compile data on cloud computing applications, information storage, and cost savings to determine possible economies of scale generated by cloud computing,

3. Officials should clarify procurement rules to facilitate purchasing through measured or subscription cloud services and cloud solutions appropriate for low, medium, and high-risk applications,
4. Countries need to harmonise their laws on cloud computing to avoid a “Tower of Babel” and reduce current inconsistencies regarding privacy, data storage, security processes, and personnel training, and
5. Lawmakers need to examine rules relating to the privacy and security of cloud computing to ensure safeguarding of information in the system.

## CHAPTER 3: METHODOLOGY

### 3.1 Introduction

This chapter presents the research design and the research methodology that was used in this study. It also outlines the research strategy, data collection techniques, sampling and data analysis techniques used to achieve the research objectives. The chapter map presents the order followed in this chapter.



### 3.2 Research Strategy

According to Saunders, Lewis and Thornhill (2009), a research strategy implies the approach used to answer the research questions and achieve the research objectives. Research strategies vary from research approach, which can be either interpretivist or positivist and the research method choice of quantitative or qualitative (Sekaran & Bougie, 2009).

This study adopted a qualitative research method because of its uniqueness to naturally describe social phenomena and to gain full understanding of the social world (Bryman,

2012; Silverman, 2013). The interpretivist approach to this research was on the assumptions that the participants answer in a subjective way, while understanding their motives and the subjective reality of the objectives (Saunders, Lewis & Thornhill, 2016). The study used a case study strategy, which aimed to explore and to develop a more comprehensive understanding of the subject being studied (Stake, 1994). A multiple-case strategy was applied within the case study because of its occurrences to generalise to other cases within the Namibian government (Patton, 2001). To understand the in-depth exploration and to achieve the objectives of this research, qualitative data collection methods such as interviews, questionnaires and literature review were used (Yin, 2014). Qualitative data analysis enabled the identification of the framework components and a more detailed understanding of the case.

The study also incorporated the design science research (DSR) strategy to develop the framework, as stipulated in the research's main objective, which is to propose a secure cloud adoption framework in the Namibian government IT departments. DSR is a "problem-solving strategy that aims at building and evaluating artefacts to address phenomena" (Bhunu Shava, 2015).

### **3.3 Design Science Research Strategy Overview**

Hevner and Chatterjee (2010) describe DSR as a paradigm that is highly significant to information technology systems for evaluation and iteration within research projects. DSR addresses two of the discipline key issues directly: the central, although controversial, role of the IT artefacts in information systems (IS) research and the perceived lack of professional relevance in research design (Hirschheim & Klein, 2003). As supported by Simon (1996) DSR cater for innovative artefacts to solve real-world problems.

Thus, this study tackled a solution by deploying DSR to develop a framework for the cloud adoption in the Namibian government IT departments. Peffers, Tuunanen, Rothenberger and Chatterjee (2007) concur that DSR contributes by "providing a commonly accepted framework for successfully carrying out DSR research and a mental model for its presentation".

According to Peffers et al. (2007), DSR also assists in presenting objectives, processes and outputs in a commonly understood framework. In the next section, the study applied the DSR six guidelines design elements by Hevner and Chatterjee (2010) to conduct and evaluate the framework process of the study.

Several researchers (Rossi & Sein, 2003 and Hevner, et al., 2004) provided some common collective guidelines to assist in carrying out the design science research methodology process in areas such as engineering, computer science and information systems (IS).

As summarised by Peffers et al. (2007), these researchers concurred on six common DSR design elements which are: problem identified and motivation, objectives of a solution, design and development, demonstration, evaluation and communication, as shown in Table 3-1.



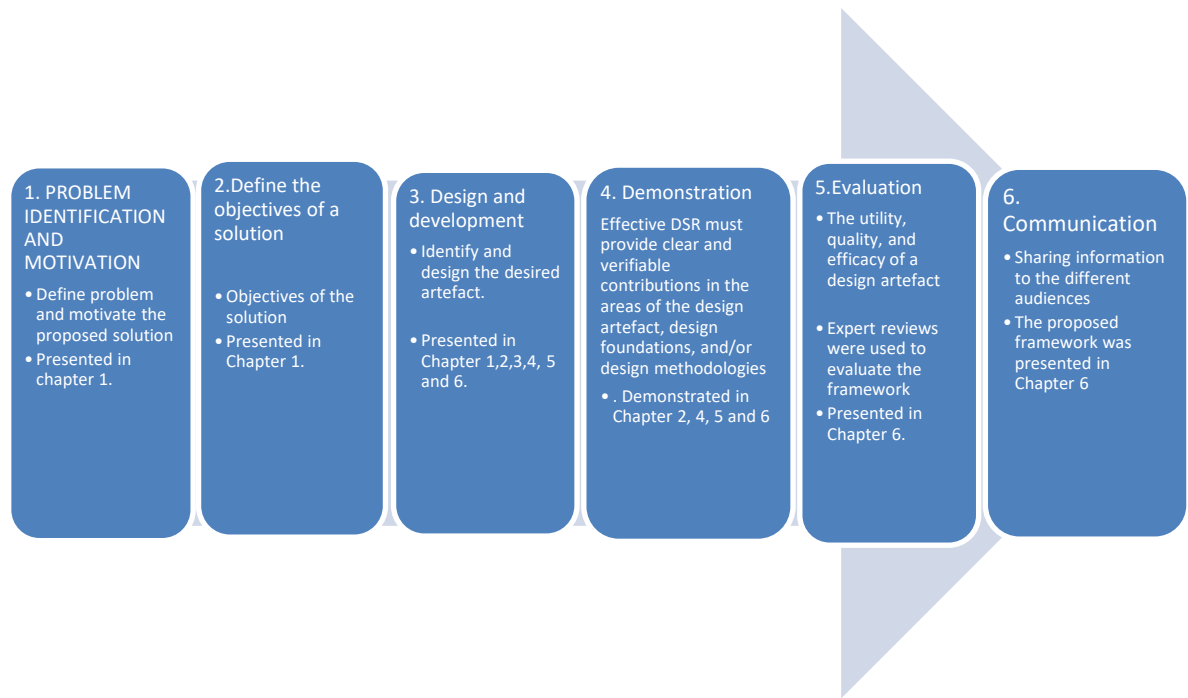
**Table 3-1: Design Science Research Elements (Source: Peffers et al., 2007)**

Common design process elements	Archer, (1984)	Takeda, Veerkamp, and Tomiyama, Yoshikawam, (1990)	Eekels and Roozenburg, (1991)	Nunamaker, Chen, and Purdin, (1991)	Walls, Widmeyer, and El Sawy, (1992)	Rossi, and Sein, (2003)	Hevner, March, and Park, (2004)
1. Problem identification and motivation	Programming Data collection	Problem enumeration	Analysis	Construct a conceptual framework	Meta-requirements Kernel theories	Identify a need	Important and relevant problems
2. Objectives of a solution			Requirements				Implicit in "relevance"
3. Design and development	Analysis Synthesis Development	Suggestion Development	Synthesis, Tentative design proposals	Develop a system architecture Analyse and design the system.  Build the system	Design method  Meta design	Build	Iterative search process Artefact
4. Demonstration			Simulation, Conditional prediction	Experiment, Observe, and evaluate the system			
5. Evaluation		Confirmatory evaluative	Evaluation, Decision, Definite design		Testable design process/product hypothesis	Evaluate	Evaluate
6. Communication	Communication						Communication

The study used these six phases to design the framework.

### 3.3.1 Mapping DSR characteristics with research objectives

This study followed the DSR guidelines informed by previous studies (Hevner et al., 2004) to map the DSR characteristics to the research objectives, which involved designing artefacts to solve problems identified within the Namibian government IT departments, make the research contributions to identify the research framework components, evaluate the framework components and design the framework and lastly the outcome results will be presented as a framework to the respective audiences (Hevner et al., 2004). Figure 3-1 presents the Design Science Research applied to achieve the research objectives.



**Figure 3-1: Design Science Research Guidelines (Source: Hevner et al., 2004)**

Below the study details the application of DSR framework design process in phases:

## **Phase 1: Define Identification and motivation**

Hevner et al. (2004) stress that DSR addresses or solves a problem in a unique, innovative, effective and efficient ways. Guideline one focuses on the identified research problem and value justification of the solution (Peffer et al., 2007). Below is the research study statement of the problem, described as the artefact.

**While traditional IT infrastructure faces low server utilisation, fragmented demand, expensive to maintain and systems that are difficult to manage, cloud computing has the potential to improve government service delivery, reduce operating costs, increase data centre efficiency and server utilisation. The study investigates the benefits and challenges associated with cloud-based infrastructure services and propose a secure framework to adopt cloud computing in the Namibian government IT departments.**

## **Phase 2: Defines the objectives of a solution**

At this stage, the study defined the objectives of the solution from the problem definition. To address the problem identified in phase 1, the following research objectives needed to be achieved:

**The aim of this study is to assess and investigate the benefits and challenges associated with adopting a cloud-based Infrastructure service, readiness to adopt cloud computing and propose a framework for secure cloud adoption in the Namibian government IT departments.**

Specific objectives:

- To analyse the cloud computing benefits for Namibia's government IT infrastructure and propose the best approach for adoption.
- To analyse security issues and challenges in adopting cloud based IaaS in Namibia's government institutions and propose secure solutions.
- To assess the Namibian government IT departments' readiness to adopt cloud computing.

- To propose a secure framework on how Namibian government can position itself to adopt to the cloud with minimum security risks.

### Phase 3: Design and development

At this stage, different components identified in the literature review and primary data were consolidated to define and develop the framework.

The identified components, which were consolidated to develop a framework, consisted of the adoption factors, process, security controls, implementation guidelines and cloud adoption evaluation. The adoption factors are needs assessment, awareness, budget, governance, executive buy in, return on investment (benefits), policies and regulations, infrastructure compatibility, bandwidth, trust, knowledge and skills, privacy and security, performance and service delivery. These adoption factors were further grouped into four categories namely: technological enablers, users' characteristics, organisational and environmental factors.

Other researchers (Takeda et al., 1990; Herver et al., 2004; Peffers et al., 2007) describe this stage as design and development, noting that this includes determining "the artefact's desired functionality and its architecture and then creating the actual artefact" (Peffers et al., 2007), while Herver and Chatterjee (2010) describe it as design evaluation. Herver and Chatterjee (2010) motive that the "utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods". This section, based on the study findings, details the framework identified components and the evaluation of these components. Table 3-2 presents the identified framework components of this study according to the TOE framework guideline.

**Table 3-2: Framework Components**

Technological	Organisational	Environmental
Cloud Benefits	Return on Investments (Budget) -Cost	Governance issues -License management -Political interferences -Corruptions

Performance -Scalability -Reliability -Bandwidth -Availability/Downtime	Challenges	Political bureaucracy
Compatibility - Infrastructure: Integration with other services	People -Trust -Skills	Policies and regulations
Security -Infrastructure security -Data security -Access security -Privacy		Service Providers -Trust -Skills

This section will be covered in detail in Chapter 6.

#### **Phase 4: Demonstration**

This phase demonstrates whether the proposed Secure Cloud Adoption Framework (SCAF) can solve the Namibian IT departments' problems. This study used a case study to use the artefact to solve the problem.

Chapter 6 demonstrates the application of the framework by using scenarios, literature and validation.

#### **Phase 5: Evaluation**

At this stage, the study demonstrates the applicability of the framework to the problem domain. The study conducted expert reviews to evaluate the SCAF framework. This study drew experts from diverse but related fields within the study area. The experts were chosen based on their expertise; and an evaluation tool was designed and developed using Google forms for evaluation purpose. The experts evaluated the framework; and their inputs were used to modify and refine the framework.

This section is covered in-depth in Chapter 6.

## **Phase 6: Communication**

The finalisation of the framework will be detailed in Chapter 6. The study findings will be shared with other researchers, as well as where the study took place.

### **3.3.2 Quality of the framework**

Rigour of the research can be established through the demonstration of the validity and reliability of the research. Care was taken throughout the design phase to ensure that the process demonstrated construct validity, internal validity, external validity, objectivity and reliability. Construct validity requires the researcher to use the correct measures for the concepts being studied. Internal validity demonstrates that certain conditions lead to other conditions and requires the use of multiple pieces of evidence from multiple sources to uncover convergent lines of inquiry. External validity reflects whether the findings are generalisable beyond the immediate case; the more variations in places, people, and procedures that a case study can withstand and still yield the same findings; the more external validity exists. Techniques such as cross-case examination and within-case examination, along with literature review, help to ensure external validity. Objectivity is the degree of independence from a researcher's bias. Reliability refers to the stability, accuracy, and precision of measurement. The procedures used are well documented and can be repeated with the same results (Yin, 2014; Dooley, 2002; Oates, 2012). Expert reviews validated and refined the framework.

### **3.3.3 Validity and Reliability**

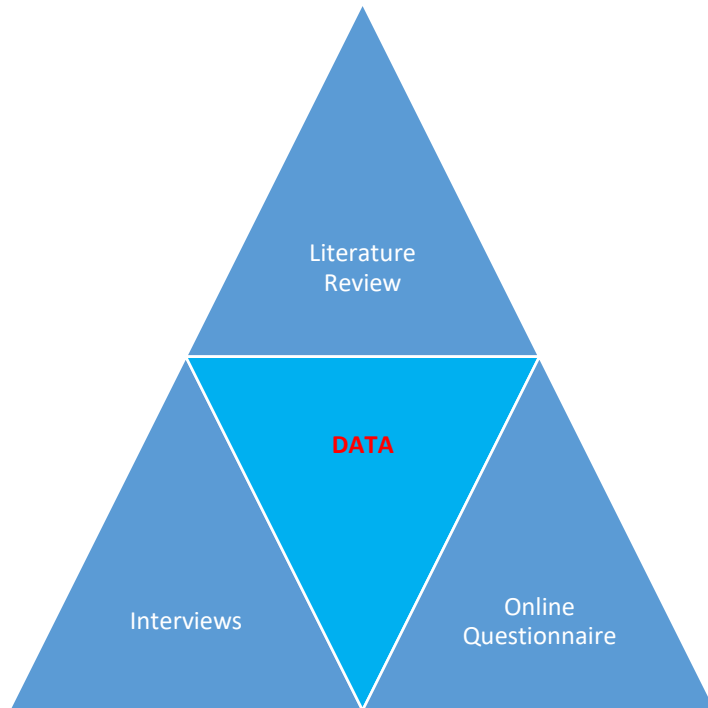
This study used an open-ended questionnaire and semi-structured interviews. The questionnaire was structured to ensure that all participants understand the aim of the study and covered a wide range of the study aspects such as cloud benefits, IaaS and SaaS adoption, security issues, challenges, awareness and usage fervour and to ensure that different views are included and respected. The questionnaire was also to discover the in-depth understanding of Namibian government IT departments on the cloud adoption and its readiness. Before the deployment of the questionnaires, a pre-test was conducted on five experts within the domain of the research study to measure the accuracy and reliability of the questions. The pre-test was also done to ensure content and construct validity. A few questions were amended after the pre-test feedback. Due

to small number of IT personnel of the sample institutions (OPM, MURD and RCs), the online questionnaire survey was designed to collect information from all IT officials.

The interviews were conducted on 10 participants shortly after the completion of the questionnaires. Participants were randomly selected based on the study population size of those who had previously filled in the study questionnaire. To ensure equal chance for despondence's participation in the face-to-face survey, each of the 25 respondents were allocated a number on a piece of paper and all papers with respondents' numbers were placed in a container mixed and thirteen respondents were identified. Appointments were made with 13 identified respondents, however only ten were available for the interviews. Participants were also informed prior to conducting the interview and confirmed their availability. Permission was also granted by the participants to be recorded. Participants were introduced to the main objective of the study, the purpose of the interview and what was expected of them. To validate and ensure accuracy of the results, participants were encouraged to be honest. The interview questions addressed the research study objectives and provided a deeper understanding of some of the answered questions previously in the questionnaire. The interview focused on the following themes: maximise service delivery, cloud adoption challenges, security risks, cloud computing as a future IT model, recommendation towards cloud adoption, IT policies and regulations and regulations towards cloud adoption, and lastly cloud infrastructure governance.

### **3.4 Data Triangulation**

Bryman (2013) defines triangulation as using two or more methods or techniques to collect data. This is to ensure validity of the research. Krauss and Putra (2005) added that triangulation captures a more comprehensive holistic content of the research process and explains the richness of details of the same phenomenon from different dimensions. This study used data triangulation using literature review, questionnaire and interviews as shown in Figure 3-2. This was done to strengthen and validate the research findings. This also ensured the verification and consistency of the study findings. Moreover, insight and understanding of the research topic was achieved through the triangulation of the multiple data collection methods, as detailed in the next section.

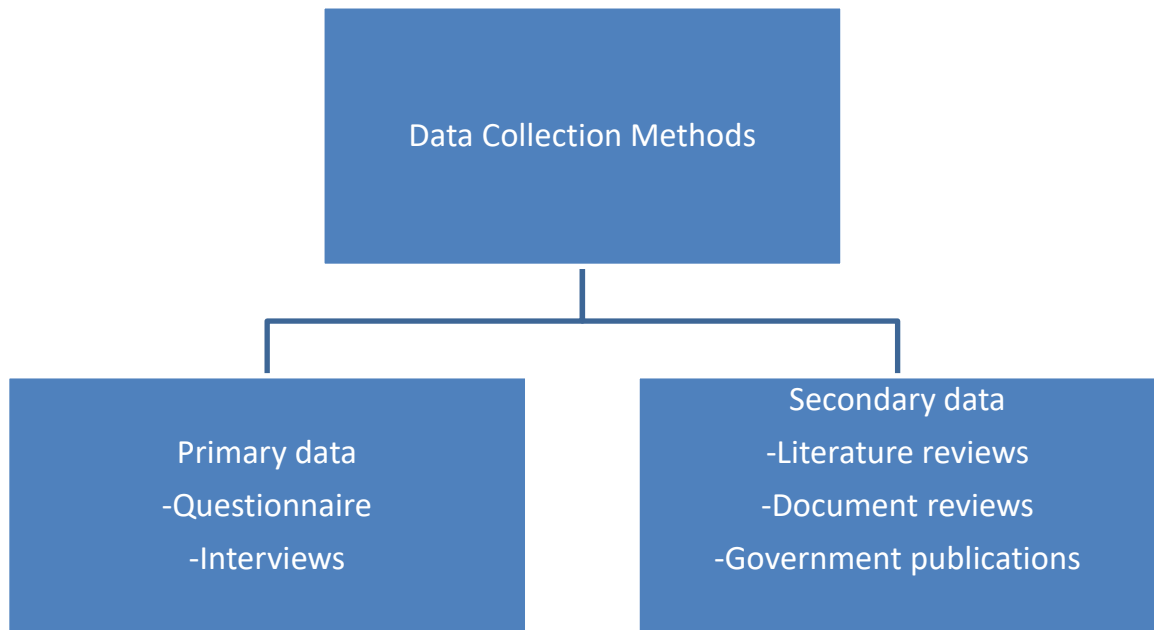


**Figure 3-2: Data Source Triangulation**

### **3.5 Data Collection**

The adoption of cloud services (IaaS and SaaS) in IT departments has not been researched yet in the Namibian government and to understand the in-depth exploration and to achieve the objectives of this research, qualitative data collection methods such as interviews, questionnaires, case materials, literature review and documentation (Oates, 2012) were used. The data collection process is an important step and the fundamental element of any research (Monton, 2001). Olivier (2009) suggests that a case study can use any of the abovementioned qualitative data collection methods. The primary data collection techniques used in this study were online questionnaire and semi-structured interviews. Literature review and documentation review were consulted as secondary data collection techniques, as summarised in Figure 3-3.





**Figure 3-3: Data Collection Methods**

### **3.5.1 Primary data**

According to Hox and Boeije (2005), primary data implies data collected for the first time by the researcher through direct efforts, experience and to address the research problem. Data can be collected through different methods such as surveys, observations, interviews, questionnaire, focus groups and interviews. Primary data for this study were collected through questionnaires and semi-structured interviews.

#### **3.5.1.1 Questionnaire**

Questionnaire is defined as a set of predefined questions assembled in a specific order (Oates, 2009). According to Creswell and Clark (2007), questionnaire can either be structured (closed-ended questions) or semi-structured (opened-ended questions). This study used a semi-structured questionnaire. The questions were structured to ensure that all IT departments participating understand the aim of the study, the questionnaire covered a wide range of the study aspects such as cloud benefits, IaaS and SaaS adoption, security issues, challenges, awareness and usage fervour and to ensure that

different views are included and respected. The questionnaire was also to discover the in-depth understanding of Namibian government IT departments on cloud adoption (Nghihalwa & Bhunu Shava, 2018).

Before the deployment of the questionnaire, a pre-test was conducted on five experts within the domain of the research study to measure the accuracy and reliability of the questions. The pre-test was also done to ensure content and construct validity (Oates, 2009). A few questions were amended after the pre-test feedback. Questionnaires were distributed to 30 participants through a self-administrative online questionnaire.

The next subsection illustrates interviews as another primary data collection technique.

### **3.5.1.2 Interviews**

Interviews are the oral questioning of individuals or a group (Denscombe, 2003). Interviews can be structured, semi-structured and unstructured. In a structured interview, the interviewer compiles and prepares the questions in advance. In a structured interview, the interviewer standardises the order in which the questions are asked, hence maintains the same context. All responses are evaluated using the same rating scale and standards for acceptable answers (Welman, Kruger & Mitchell, 2005). Secondly, in an unstructured interview, also referred to as an informal interview or discovery interview, the interviewer starts by introducing the topic and lets the interviewee's ideas flow. It contains open-ended questions and can be asked in a particular order (Oates, 2006). While Vanderstoep and Johnston (2009) define a semi-structured interview as a technique that has both structured and unstructured properties. The interviewer follows a list of questions and themes to be covered during the conversation and in a particular order.

This study conducted semi-structured interviews on 10 participants shortly after the completion of the online self-administered questionnaires. Participants were randomly selected based on the study population size of those who had previously filled in the study questionnaire. Participants were also informed prior to conducting the interview and confirmed their availability. Permission was also granted by the participants to be recorded. The interaction between the participants and the interviewer was face to face. Participants were introduced to the main objective of the study, the purpose of the

interview and what was expected of them. To validate and ensure accuracy of the results, participants were encouraged to be honest.

The interview questions aimed to address the research study objectives, get a deeper understanding of some of the answered questions in the questionnaire as well as to validate the framework components. The interview focused on the following themes: maximise service delivery, cloud adoption challenges, security risks, cloud computing as a future IT model, recommendation towards cloud adoption, IT policies and regulations and regulations towards cloud adoption, and lastly cloud infrastructure governance.

The next section describes the secondary data collection technique.

### **3.5.2 Secondary data**

Secondary data implies the second-hand information which is already collected or produced by others (Hox & Boeije, 2005). This data is recorded by other researchers, for purposes not related to the current research problem. It is readily available from sources like literature review, books, reports, documentation, government publications, websites, journal articles, etc.

This study consulted literature review, documentation, government publications and journal articles as secondary data.

#### ***3.5.2.1 Literature review, documentation and government publication***

Lastly, documentation containing useful and very important information was gathered. Literature of governments, which have implemented and adopted cloud-based services, was reviewed to strengthen the findings and to act as a guideline to the formulation of the proposed solution model.

### **3.6 Sampling**

According to Nastasi (2004), sampling refers to the selection of settings (individuals, units, process, event, etc.) to be studied, which is either purposeful or criterion-based, and it is characterised according to the research objectives. This study used a multiple

case strategy (typical and critical case sampling) applied within the case study because of its specific occurrences strata within the main case.

Typical case sampling focuses on what is “typical, normal and average” while critical case sampling will “permit logical generalisation and maximum application of information to other cases because if it is true of this one case, it is likely to be true of all other cases” (Patton, 2001). According to Mitchell (2000), the logical generalisation of a case study reflects the substantive of the topic or issues of interests.

According to Nghihalwa and Bhunu Shava (2018), OPM and MURD were used as a case study out of the Namibian government OMAs because OPM facilitates and approves new technologies. MURD consists of regional council offices and constituency offices around the country. This is like most of the Namibian government OMAs, which have support offices in the regions, in line with e-government to bring services closer to all Namibian people. In light of the above, it was assumed that MURD would produce critical information, which was typically significant in achieving the objectives of this study. Yin (2014) emphasised that having multiple case strategies strengthens the findings of the entire study, because of the presumed replications of the same phenomenon.

The case study is presented in more detail in Chapter 4. The next section discusses the data analysis of the study.

### **3.7 Data Analysis**

Analysis of data entails summarising data collected and presenting the results in a form that communicates the objectives of the study (Bryman, 2012). The study analysed the data using qualitative content analysis. Hsieh and Shannon (2005, p.1278) define qualitative content analysis as a “research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns”.

Previous studies (Zhang & Wildemuth, n.d.) compare and contrast qualitative content analysis to quantitative content analysis and describe qualitative content analysis as focusing more on exploring the meanings underlying physical messages. While quantitative content analysis uses more of probabilistic approaches, qualitative content

analysis consists of purposively selected texts which can inform the research questions being investigated.

Although qualitative content analysis focuses more on inductive reasoning using themes and categories that emerge from the data through the researcher's careful examination and constant comparison (Zhang & Wildemuthn, n.d.), Patton (2001) reasons that it does not exclude deductive reasoning where it is useful to generate concepts and variables from theory or previous studies.

There are three approaches to inductive reasoning in qualitative content, namely, conventional qualitative content analysis, directed qualitative content analysis and summative qualitative content analysis says Hsieh and Shannon (2005). This study used the directed qualitative content analysis approach, in which initial coding started with other theory and relevant research findings, then, during the data analysis the researcher immersed into the data and allowed themes to emerge from the data. By this approach, the framework components were validated and the framework was refined thereof.

The steps to analyse qualitative data are as follows: data preparation, data reduction, data categorisation, identification of patterns and themes, data display and draw conclusions (Creswell, 2013 & Schreier, 2012) and depicted in Table 3-3 as followed in this study.

**Table 3-3: Data Analysis Process**

	Steps	Description
Step 1	Data preparation	Data was prepared for analysis by coding each question and each response was given a unique number.  The data of the interview were transcribed into text before the analysis.
Step 2	Define the unit of analysis	Refers to the basic unit of text to be classified during analysis. The study identified three main context units of analysis namely: organisational, technological enablers and environmental.
Step 3	Develop categories and a coding scheme	Categories and the coding scheme were derived from related studies and the research data. Categories were developed inductively from an initial list of coding and the list was modified as new categories emerged inductively during analysis.

Step 4	Test your coding scheme on a sample text	At this stage, the coding scheme was tested on sampled data to check for consistency and errors.
Step 5	Code all the text	After checking for consistency, the data were coded and new themes such as political interference and corruption were added to the list.
Step 6	Assess your coding consistency	After coding the entire set of data, another consistency check was performed on the overall coding.
Step 7	Draw conclusions from the coded data	This is the most crucial step in data analysis. This step involved making sense of categories, identifying relationship between categories and uncovering patterns.
Step 8	Report methods and findings	Meaningful data were presented in charts, tables and frequently used words based on the research questions.

According to Hancock (2002), qualitative research is fundamentally interpretive, and interpretation analysis is more “concerned with what was meant by the response, what was inferred or implied”; hence it was ideal for analysing the questionnaires and interviews to get the participants’ views and opinions on the adoption of cloud IaaS services and its security issues and challenges.

### 3.8 Unit Analysis

Unit analysis signifies data collected and helps to define the types of data to collect and from which right institutions to collect data from (Barratt, Choi & Li, 2011). This research targeted the IT personnel from OPM, MURD and RCs. The IT staff consisted of seniors’ staff such as deputy directors, chief and senior systems administrators and analyst programmers and junior staff such as system administrators, analyst programmers and technicians. Senior staff were highly considered because of their involvement in planning and budgeting for IT infrastructure. Technical personnel were valued as they had greater influence on the adoption of cloud services, thus contributing to the effectiveness of data collection.

### 3.9 Research Ethics

Participation in the study was voluntary. The results of this research are reported correctly. Participants were presented with research objectives. Data collected during this research were used for the purposes of this study only.

### 3.10 Anonymity and Confidentiality

The users were kept anonymous. Findings were treated in a confidential manner ensuring that, upon reporting or publishing, no link can be made to the population studied. No personal information was gathered, hence the privacy of participants was not violated.

### 3.11 Chapter Summary

Chapter 3 described the methodology used for this research. The chapter demonstrated methods employed in achieving the research objectives. Qualitative research method was used in a case study. Data collection techniques such as questionnaire, interviews and literature review was used. Design science research method was used to develop the framework. The chapter further discussed sampling, data analysis and ethical considerations. Case study, detailed research findings and discussions are presented in the next chapters. The next chapter presents the case study.

Table 3-4 summarises the research methodology:

**Table 3-4: Research Methodology Summary**

Research Aspects	Research options
Research Choice	Qualitative
Research Paradigms	Design Science Research, Interpretivist
Research approaches	Deductive
Research Strategies	Case Study (Multiple case)
Data Collection tools	Questionnaires, interviews, literature review, documentation review and expert review
Sampling	Typical case sampling,
Data Analysis	Qualitative content analysis, heuristic evaluation

Table 3-5 presents the research objectives and the data collection tools used to address the research objectives.

**Table 3-5: Research objective and data collection tools used**

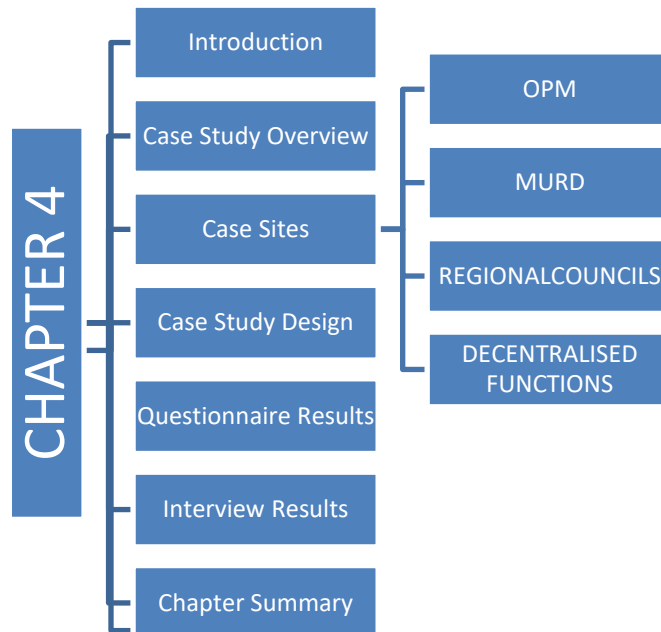
Research Objectives	Data collection Method used
To analyse the cloud computing benefits for Namibia's government future IT infrastructure and propose the best approach for adoption.	Questionnaire, interviews, literature review
To analyse security issues and challenges in adopting cloud-based Infrastructure as a Service in Namibia's government institutions and propose secure solutions.	Questionnaire, interviews, documentation and literature review
To assess the Namibian government IT departments readiness to adopt cloud computing.	Questionnaire and literature review
To propose a secure framework on how the Namibian government can position itself to adopt to the cloud with minimum security risks.	Questionnaire, interviews, documentation, literature review and expert review



## CHAPTER 4: CASE STUDY

### 4.1 Introduction

This chapter gives an overview of the cases studied and the data collected therein. It describes the case study in detail, including the roles and responsibilities of each case. The case studies include OPM, MURD, RCs and decentralised functions. Each case's IT organisational structure is presented. This also presents the results of data collected from the case sites using questionnaires and interviews. All respondents were drawn from information technology background and have a basic insight of IT technologies adoption. The participants include IT managers (directors and deputy directors), system administrators, technicians, programmers and systems analysts. The information was organised into five components, namely: demographic results, perceived importance of IaaS and SaaS, cloud benefits, cloud security and other related issues including the challenges hindering the adoption and service delivery and accessibility. Section 4-12 details the interviews results. The chapter further discusses the case study findings. The chapter map presents the order followed in this chapter.

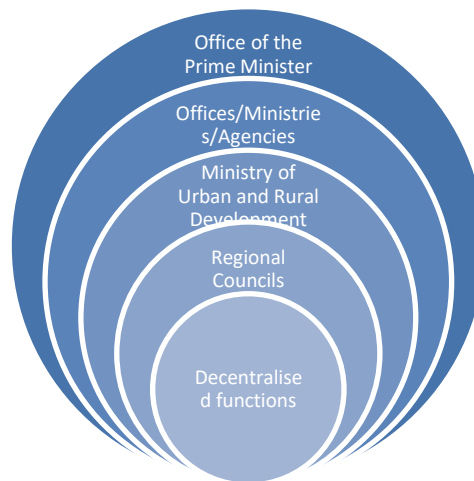


## 4.2 Case Studies Overview

Yin (2014) describes a case study as an “empirical inquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not clearly evident”. A case study approach was used to address the research objectives. OPM, MURD, RCs and decentralised functions were used as case studies as a representation of the Namibian government IT departments.

Selection of a case study depends on whether the cases are highly effective, not effective, representative, and typical or of special interest (Neale, Thapa & Boyce, 2006). Furthermore, Zucker (2009) emphasises that the reason for conducting a case study might be exploratory, descriptive and explanatory. The four government institutions were selected as a case study because of their roles, size, influences on the Namibian government IT infrastructure and the ability to replicate services within the Namibian government institutions. The next section provides the case studies’ overview in more detail.

## 4.3 Case Studies



**Figure 4-1: Association of Cases**

Figure 4-1 shows the unique relationship of the case study as described in the next sections:

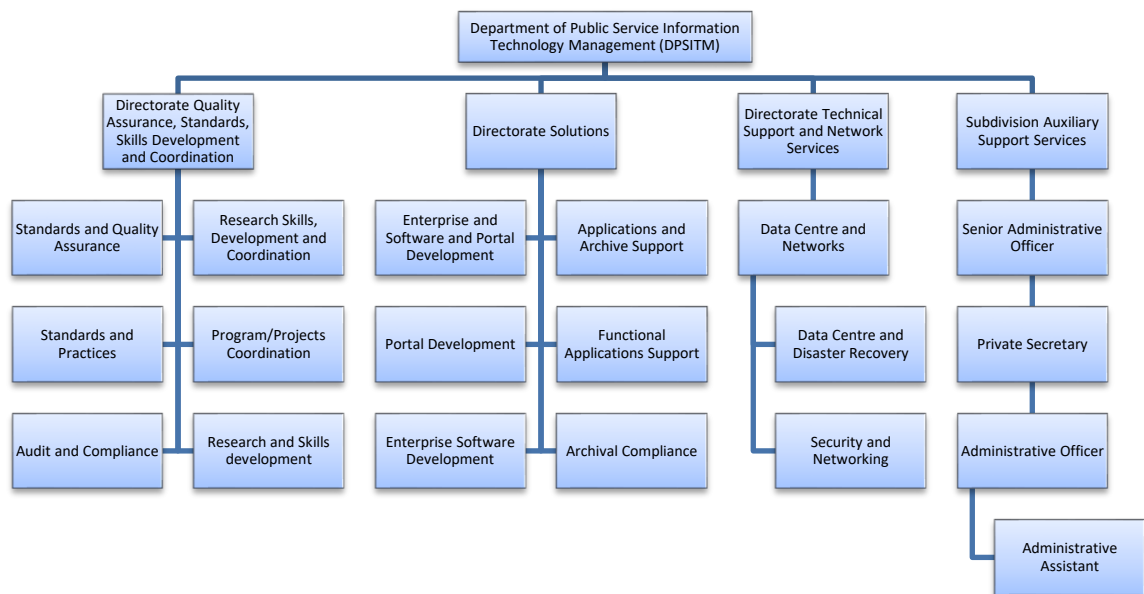
#### **4.3.1 Office of the Prime Minister**

OPM is an institution that enables the Namibian government to operate at developed country level in pursuance of Namibia's Vision 2030 (OPM, 2016). Its mandate is to lead government business in Parliament, coordinate the work of Cabinet, advice and assist the President in the execution of Government functions, oversee and manage public services and execute special projects assigned to the Office (OPM, 2016).

According to OPM (2016), OPM has two main IT departments namely: (i) Department of Administration and IT Management and (ii) Department of Public Services IT Management to keep the government on top of the latest information and communications technology developments. The main objectives of OPM IT departments are listed below:

- To provide service concerning the development and maintenance of up-to-date and viable computer information based on both political and administration matters.
- To facilitate the processes of formulation of policy and implementation of programs within the Office of the Prime Minister and the Public Service as a whole.
- To provide operational data service; develop and maintain systems; investigate Offices/Ministries/Agencies (OMAs) computer-related needs; recommend appropriate systems; control the acquisition of hardware and software in the entire Public Service through the Tender Board; draw up hardware/software specifications for the invitation of tenders and evaluates delivered goods and services (OPM, 2016)

OPM achieves these IT objectives through a departmental structure. This study focused on Public Services IT management departmental structure and the functions, role and responsibilities are illustrated in Figure 4-2:



## Department of Public Service Information Technology Management

**Figure 4-2: OPM IT Departmental Structure**

This department exists to keep the government on top of the latest information and communication technology developments for a faster and smoother flow of digital information within the government system. The department is headed by the Permanent Secretary (PS), who sets the strategic direction for the department, coordinates policy implementation and ensures the effective administration of the department through various directorates and subdivisions (OPM, 2016).

### **Directorate of quality assurance, standards, skills development and coordination**

The directorate is responsible for managing IT quality and developing IT standards, guidelines and policies for the public service (OPM, 2016). The directorate's role is to promote the acquisition of quality computer hardware and software. When all government ministries are purchasing computer hardware and software, they get specifications from this division. This is to ensure a standard model for acquiring hardware and software.

The directorate is also responsible for skills development across the ministries (OPM, 2016). They promote computer professional competency by arranging for ICT training for the IT workforce. Training and skills transfer is considered very crucial for the department and, as such, it takes up much of the department's financial budget. This is to ensure that

the IT workforce is skilful and competent enough to manage the information systems and technologies needed for achieving the ministries' objectives.

### **Programmes/project management**

Every project carried out in the ministry is assigned to a manager. The project manager is mainly responsible for the project planning, execution and control. He/she directs team members to execute the project and checks the progress of the project (OPM, 2016).

### **Standards and practices**

The department's role and responsibility is to develop IT standards and practices (OPM, 2016). The standards and practices are used to guide and maintain consistencies in the deployment of IT artefacts.

### **Audit and compliance**

The department consists of auditors and compliance officers. The department's role and responsibility is to ensure that business processes and activities comply with the defined policies, practices and standards (OPM, 2016). The auditor and compliance officers advise the ministries on the inconsistencies and irregularities occurring within their computing environments.

### **Directorate of solutions**

The directorate of solutions is responsible for the development and implementation of systems and applications (OPM, 2016). The directorate's subdivisions work closely together with applications and solutions users to get the best view of what is expected (OPM, 2016). OPM (2016) presents the directorate's subdivisions as follows:

- **Enterprise software and portal development**

The division's role is to develop and implement the various ministries' specialised applications and website portals. Therefore, one finds software developers, analyst programmers and business analysts at this division. The specialists are responsible for business and technical requirements collection and analysis needed to provide guidance for their development processes. Their work includes conceiving, designing and

maintaining databases and telecommunications integrated with other systems; translating specifications into computer language, testing results, designing or assisting in the design of file structures. Incumbents are expected to bring projects to a conclusion, including the development of operating procedures, instructions and training and the required documentation. The development of the application and information systems is done according to the pre-standards set by the quality assurance directorate.

- **Applications and archive support**

The division is responsible for managing applications, documentations and the retrieval and archiving of documents in the organisation.

### **Directorate of technical support and network services**

The technical support and network services directorate manages the subdivisions responsible for the computer hardware implementation, troubleshooting and maintenance of the Internet and network services in the ministries. The directorate's purpose is to ensure that the technical infrastructure acquired meet the specifications and standards defined. The directorate's mandate is carried out through the following subdivisions:

- **Data centre and disaster recovery**

The division is concerned with data management as well as the recovery of the organisational data. Daily, organisations face challenges from natural disasters as well as viruses and other intentional attacks that could be threats to their data and information. Hence, the division's responsibility is to ensure that backup systems are in place and operational.

- **Security and networking**

The security and networking subdivision is responsible for managing networking security in the organisation. It ensures that the network connections are up and running and they are secure and reliable to support communication and collaboration activities. The subdivision employs network administrators and network specialists to realise its objectives.

- **Division of auxiliary support and services**

The division consists of administration officers and their respective secretaries. The division is responsible for the IT division enquiries, processing, attending to incoming calls, filing divisional documents and ensuring that the departmental administrative stationeries are at hand.

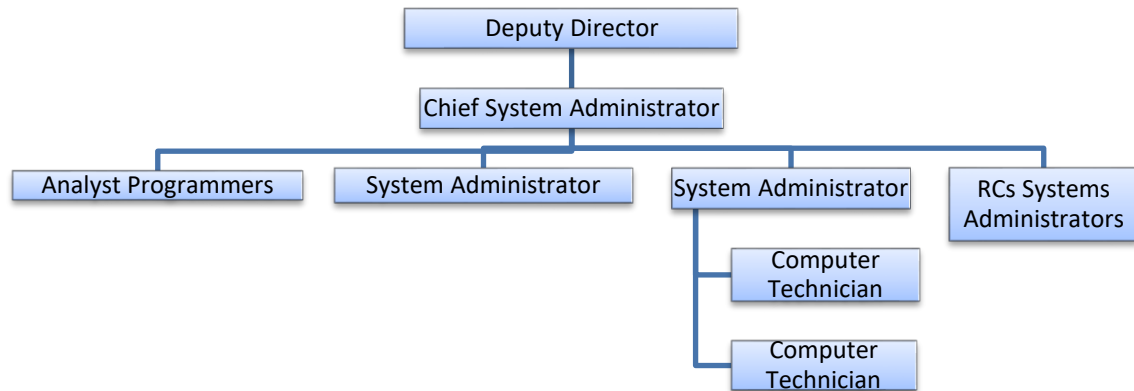
#### **4.3.2 Ministry of Urban and Rural Development**

MURD is one of the ministries that fall under the OPM. MURD's mission is the delivery of services to the satisfaction of all communities through rural development, establishment of an effective, decentralised regional and local government system, housing and physical planning. The ministry has the role to coordinate and spearhead the decentralisation process (MURD, 2016). The main aim of the ministry is to ensure economic, cultural and socio-economic development, giving people at the grassroots level the opportunity to participate in their own decision-making and extending democracy, give sub-national governments discretionary powers to plan, budget and implement in response to local needs, but within the framework of a unitary state.

MURD's main objectives (MURD, 2016) are as follows:

- To extend, enhance and guarantee participatory democracy.
- To ensure, enhance and safeguard rapid sustainable development.
- To transfer real power to the regional councils and local authorities based on national ideals and values.
- To improve the capacities of regional and local government councils to plan.
- Implement, manage and monitor delivery of services to their constituents.

The IT department structure of MURD is as follows:



**Figure 4-3: MURD IT Department Structure**

Figure 4-3 illustrates the following:

### **Deputy Director**

The deputy director manages the general services of all departments in the ministry, and plans and budgets for all departmental activities (MURD, 2016). The deputy director monitors the various departments' involvements in projects allocated to them and ensures that the employees carry out their tasks for departmental objectives achievement. He/she also approves all decisions in the entire department.

### **Chief System Administrator**

In the ministry, the chief system administrator's responsibility is to make sure that all IT policies are adhered (MURD, 2016). He/she manages the IT infrastructure and communicates about the IT project needs that arise in the Ministry to the OPM. Employees in the department report to the chief system administrator and he/she authorises the employees' actions. However, in the organisation, the chief system administrator reports to the deputy director. He/she is also responsible for the systems administrators in the regions.



### **System administrators**

The system administrators report to the chief system administrator. His/her responsibilities are to troubleshoot performance issues and resolve problems relating to the operation of the network. System administrators define the information systems' configuration standards for networks, file servers, application servers, computers, notebooks and software applications. They also train personnel and others on network operations (MURD, 2016).

### **Analyst programmers**

The analyst programmers are responsible for the organisation's website development and maintenance. Analyst programmers are also responsible for user requirements collection, systems and applications specifications, and documentation. They perform systems analysis and applications programming as well as assisting in the overall analysis and design of information technology systems (MURD, 2016).

### **Computer technicians**

Computer technicians support and maintain the hardware and software in the organisation. Their responsibilities include day to day computer troubleshooting, fixing computers' hardware or software and the installation of hardware and software (MURD, 2016). In the ministry, the technicians are also responsible for assisting users who have difficulties using computers.

The ministry gives IT support to 14 RCs in all 14 regions around the country. The RCs then technically support the constituency offices and decentralised functions such as the ministry of education, ministry of works and transport, ministry of health and others still to be decentralised in the remote areas (MURD, 2016). The government aims to bring service delivery closer to the people.

## **System administrator**

MURD (2016) reveals that the system administrator in the regions' responsibilities are to ensure that the network is up and running at the RC office and all decentralised offices. Attend to issues relating to the operation of the network. If a major issue arises that cannot be solved within, the problem is then escalated to the chief system administrator at MURD. The system administrator also ensures that information systems' configuration standards for networks, file servers, application servers, computers, notebooks, and software applications are adhered to. He/she supervises the computer technicians.

### **4.4 Case Study Design**

Rowley (2002) narrates that research design ensures coherence between data to be collected and conclusions to be drawn from the initial questions of the study.

The case study was purposively stratified based on the use and management of IT technology in government. Thus the study used multiple case strategies (typical and critical case sampling) applied within the case study because of its specific occurrences strata within the main case. Typical case sampling focuses on what is "typical, normal and average" while critical case sampling will "permit logical generalisation and maximum application of information to other cases because if it's true of this one case, it's likely to be true of all other cases" (Patton, 2001). According to Mitchell (2000), the logical generalisation of a case study reflects the substance of the topic or issues of interest.

To achieve the objectives of this study, Ministry of Urban and Rural Development was used as a case study out of the Namibian government OMAs. This is because MURD is the line ministry under which of regional council offices resorts while most of the other OMAs have also regional offices to avail government services closer to the community as per the government's decentralization policy. In light of the above, it is assumed that MURD will produce critical information, which is typically significant in achieving the objectives of this study (Nghihalwa & Bhunu Shava, 2018). Yin (2014) emphasises that having multiple case strategies strengthens the findings of the entire study because of its presumed replications of the same phenomenon. OPM has a significant influence in this

study because of its capacity to approve, fund and implement projects within the Namibian government.

Permission was granted to collect data from all the said government IT departments. To understand the in-depth exploration and to achieve the objectives of this research, qualitative data collection methods such as interviews, questionnaires, case materials, literature review and documentation were used.

Online questionnaires were used to discover the in-depth understanding of Namibian government IT departments on cloud adoption. Due to small number of IT personnel of the sample institutions (OPM, MURD and RCs), the online questionnaire survey was designed to collect information from all IT officials. The questionnaire were submitted to a population of 30 IT official of OPM, MURD and the 14 RCs. However, only 25 response were received.

Addition to the online questionnaire survey, a face-to-face interviews were conducted to address objective one and two, as well as to propose a secured framework for the adoption of cloud computing technology in Namibia. To ensure equal chance for despondence's participation in the face-to-face survey, each of the 25 respondents were allocated a number on a piece of paper and all papers with respondents' numbers where placed in a container mixed and thirteen respondents were identified. Appointments were made with 13 identified respondents, however only ten were available for the interviews. Hence, the respondents for face-to-face interviews were identified randomly.

Lastly, ICT policies, procedures and implementation documentation were reviewed. Literature review of governments who have implemented and adopted cloud-based services was conducted to further understand the case in context regarding cloud computing adoption. The questions for the questionnaire and interviews were set prior to data collection to maintain consistency and uniformity. Interview questions were also piloted on five participants and revised accordingly prior to data collection.

Chapter 3 described the designing process of the questionnaire and interview tools and are presented in appendices E and F, respectively.

The next section presents the study results from the case study. The results will be presented as follows:

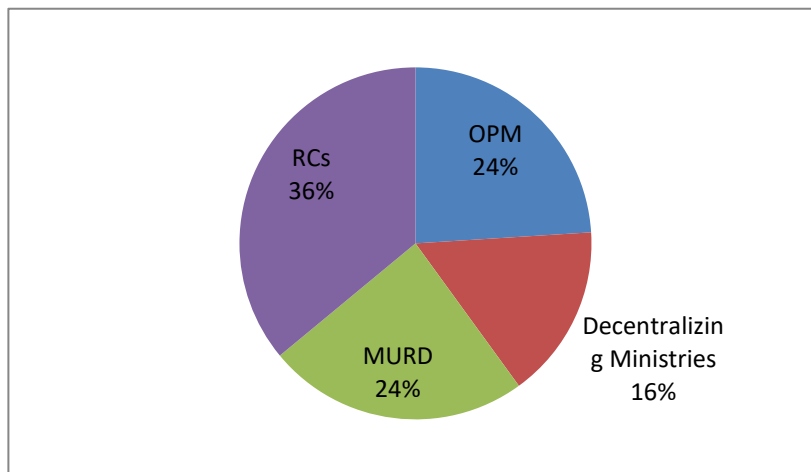
## 4.5 Demographic Results

This section details the respondents' demographic characteristics, which include: sampled government institutions and portfolios of respondents.

### 4.5.1 Sample institutions

Respondents were drawn from the Namibian government IT officials of OPM, MURD, RCs and decentralised ministries to RCs.

The study found that the majority of the respondents (36%) were from the RCs while OPM and MURD accounted for 24% each as shown in Figure 4-4. The decentralising ministries accounted for the least chunk of the respondents with 16%.

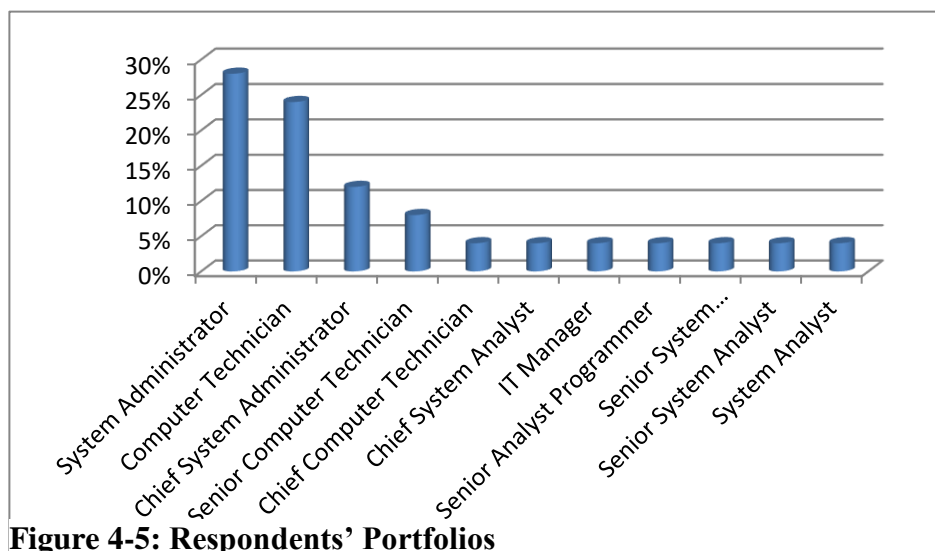


**Figure 4-4: Sampled government institutions**

### 4.5.2 Portfolios of respondents

Online questionnaires were used to discover the in-depth understanding of Namibian government IT departments on cloud adoption. Due to the small number of IT personnel of the sample institutions (OPM, MURD and RCs), the online questionnaire survey was designed to collect information from all IT officials. The questionnaires were submitted to

a population of 30 IT officials of OPM, MURD and the 14 RCs. An online questionnaire survey was designed to collect information from all IT officials, a population of 30 IT staff. However, the study only received 25 responses from government officials who deal with IT infrastructure and software, including IT managers (directors and deputy directors), system administrators, technicians, programmers and analysts as presented in Figure 4-5. According to the study, the majority of the respondents were System Administrators (28%) and Computer Technicians (24%). It is also evident from the study that the least respondents include IT managers, chief systems analyst and senior systems analyst.



**Figure 4-5: Respondents' Portfolios**

#### **4.6 Perceived importance of Infrastructure as a Service and Software as a Service**

Cloud computing is a relatively new concept in the Namibian IT public industry, hence to assess the adoption readiness, respondents were asked whether they knew cloud computing. Their responses were categorised into five responses namely: those that were very familiar, those that were familiar, those who were relatively familiar with it, just learning about it and finally those that were not familiar at all. Table 4-1 shows that most of the respondents (36%) were very familiar with the cloud computing concept, while 24% of the respondents just learnt about cloud computing concept. However, the study also revealed that 20% of the respondents were familiar and relatively familiar with cloud computing and none of the respondents were unfamiliar with the cloud computing system.

**Table 4-1: Cloud computing familiarisation**

Respondents	Level of familiarity	Notes
36%	Very Familiar	Respondents were well aware and fully understood the cloud computing implications and confident to use the technology.
20%	Familiar	Respondents were well aware of cloud computing with limited understanding and confidence to use cloud computing.
20%	Relatively Familiar	Respondents were somehow aware of the concepts, but were not sure of the implications of the technology.
24%	Just learnt about it	Respondents just heard about the cloud computing concept, but did not have much insight and understanding.
0%	Not familiar at all	Respondents were neither aware nor understood the concept of cloud computing

To assess the perception of the respondents towards cloud computing adoption in Namibian government, IT departments respondents were asked to air their views on possible benefits associated with cloud computing.

The study (Table 4-2) found that over 31% of the respondents appreciated the use of IaaS and SaaS cloud, stating that it improved service delivery. About 23% of the respondents acknowledged the advanced IT infrastructure that cloud brings forth, while 11% of the respondents felt that the technology saved cost. About 11% of the respondents perceived that cloud computing would enhance the availability of information, while the other 11% of the respondents viewed the paradigm as increasing performance and storage capacity. The other perceived benefits of cloud were flexibility and secure backup. In total response, seven out of eight issues categories listed were positive representing about 87% of benefits and non-benefits were grouped from the respondents' comments as quoted and identified from the respondent's comments in Table 5-3. Positive perception implies that respondents are in favour of the perceived benefits from cloud adoption and the positive attributes associated with cloud. While

negative perception implies that respondents are unsure of what the technology/concept entails.

**Table 4-2: Perceived importance of IaaS and SaaS to Namibia**

Description of the Perception	Respondents	Attitude notes (Positive and Negative Perception)
Improved service delivery	31%	Positive perception: in favour of the perceived benefits towards cloud adoption and the positive attributes associated with cloud.
Advanced IT infrastructure	23%	
Availability of information	11%	
Saves cost	11%	
Increased performance and storage capacity	9%	
Secure backup	6%	
Flexibility	6%	Negative perception: unsure of what the technology/concept entails.
Unsure	3%	

Table 4-3 presents some of the comments from the respondents.

**Table 4-3: Comments from respondents**

- ❖ *“Think it will be great but I am concerned with the security “*
- ❖ *“It could mean availability of information at all times in terms of portability, security and backup of data made easy. No need to back up or worry if anything happens to your PC/laptop, all the data will be intact. However, there is always security concerns regarding data saved on cloud, especially the GRN data. Issues like confidentiality of data, etc.”*
- ❖ *“It means risking the government data”*
- ❖ *“It will help to reduce physical infrastructure”*
- ❖ *“Advancing technology”*
- ❖ *“It will be beneficial, eases access to software, well supported infrastructure but it will also mean putting in place IT security measures since it’s Government where policy need to govern how cloud computing is deployed and utilised.”*
- ❖ *“This could mean less spending on the main IT hardware (like servers) and software.”*
- ❖ *“Central storage, improves accessibility of information”*
- ❖ *“The cost of IT infrastructure is reduced and its uptime is increased. The government will no longer have the responsibility of ensuring uptime, maintaining hardware and networking equipment, or replacing old equipment. IaaS has the ability to scale up and down quickly in response to an enterprise’s requirements. Government has the ability to accelerate the delivery of product/service to its citizens. Less time is spent on backups and the need to spend on the introduction of new underlying software, time spent on installing/ downloading patches for upgrades or updates. It can keep IT costs consistent or lower than packaged or home grown software.”*
- ❖ *“Bringing service to the people in a timely manner”*
- ❖ *“Improved service delivery to the public through the use of improved computer resources.”*
- ❖ *“With IaaS, it would mean less money spent on physical infrastructure upgrades and cost on both hardware replacements and troubleshooting as well as less people resources, technical people needed to troubleshoot the physical infrastructure. However, it is still a risk on security as there is no control on the physical (geographical) location of the VM, and I don’t believe it’s in the best interest for the government to not know or dictate where to keep its data.”*  
*“Improved hardware utilisation and centralised IT; eliminates problems currently faced with lack of proper IT support companies in the regions”*

#### **4.7 Cloud Benefits**



Respondents were asked what their perceptions were on the benefits cloud computing has over the current traditional IT infrastructure. Furthermore, based on the cited/identified benefits, they were requested to rank, in order of importance to OPM, MURD, RCs and/ or decentralised functions, cloud benefits such as increased collaboration, pricing flexibility, no upfront investment, convenience for the development teams, IT efficiency, ability to grow and shrink, IT capacity on demand, new products and services, operational cost savings, software cost savings, hardware utilisation, improved security, better functionality, complexity reduction, better scalability and more flexibility and centralised IT. The following sections present the findings. These findings are to address the study's first objective, which is to analyse the cloud computing benefits for the Namibian government future IT infrastructure.

#### **4.7.1 Perceived Cloud Benefits Over Traditional IT Infrastructure**

Respondents were asked to express their opinions on the benefits cloud computing delivery services (IaaS and SaaS) have over the current traditional IT infrastructure. These benefits of cloud-based infrastructure over traditional IT infrastructure are viewed as positive perception because of their positive contribution towards cloud adoption in the Namibian government.

Regarding the perceived benefits of cloud computing over traditional IT infrastructure, 100% of the respondents listed positive benefits of the technology and there were no negative issues associated with the technology. Furthermore, nearly half of the respondents (44%) cited cost effectiveness as the most perceived benefit (Table 4-4). Some of the respondents cited that cloud services would reduce government cost as indicated in Table 4-4. Up to 20% of the respondents appreciated centralised resources, while 16% valued the easy accessibility of the paradigm. Lengthy procurement process reduced, hardware utilisation and efficiency were cited by 12% as some of the benefits highlighted in Table 4-4. Data recovery and backup (8%), improved storage space (8%), IT experts reduced (4%), flexibility (4%) and solved security issues (4%) were appreciated by a few.

**Table 4-4: Perceived cloud benefits over current IT wired infrastructure**

<b>Perceived cloud benefits over traditional IT infrastructure</b>	<b>Respondents</b>
Cost effective	44%
Centralised resources	20%
Easily accessible	16%
Hardware utilisation	12%
Efficient	12%
Lengthy procurement process solved	12%
Improved storage space	8%
Data recovery and backups	8%
IT experts reduced	4%
Flexibility	4%
Solved security issues	4%

#### **4.7.2 Importance of cloud benefits**

In addition to the benefits identified by the respondents, other authors presented up to 15 benefits associated with cloud computing.

For this study, respondents were engaged to confirm and rank the benefits according to the following:

1. Not important
2. Slightly important
3. Important
4. Very important
5. Extremely important

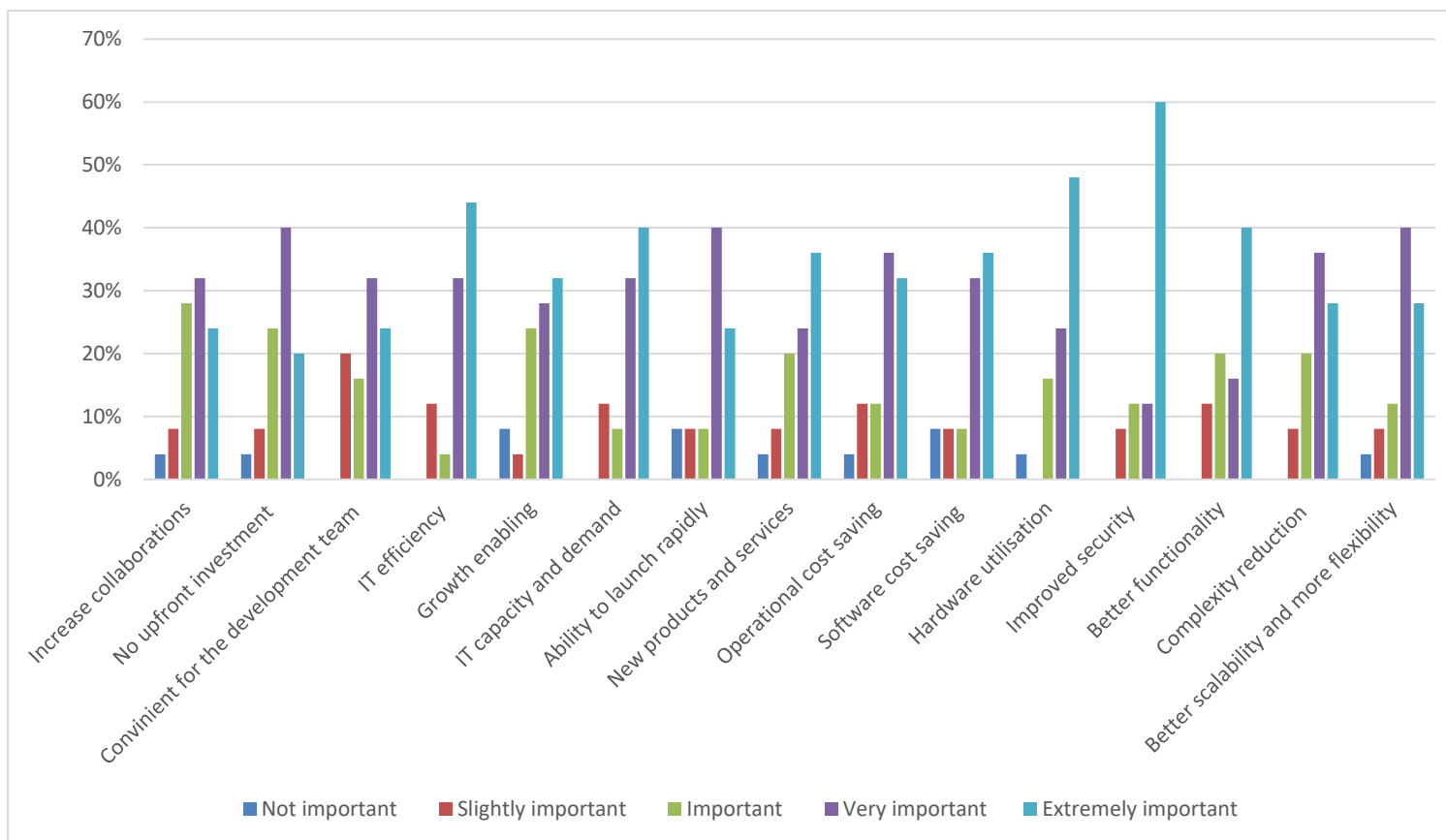
On average, 37% of the respondents appreciated cloud computing ranking the benefits as extremely important, an average of 33% ranked the cloud paradigm benefits as very important and 17% as important. On average, only 3% of the respondents perceived cloud computing as not important as shown in Figure 4-6. In view of ranking the cloud

benefits, Figure 4-6 also illustrates that the following benefits were mostly perceived as extremely important by many respondents:

1. Improved security (60%)
2. Hardware utilisation (48%)
3. IT efficiency (44%)
4. IT capacity and demand (40%)
5. Better functionality (40%)

In addition, most of the cloud computing benefits were ranked very important and, as shown in Figure 4-5, these include:

1. No upfront investments (40%)
2. Better scalability and more flexibility (40%)
3. Ability to launch rapidly (40%)



**Figure 4-6: Importance of cloud benefits**

#### 4.8 Cloud Security and Other Related Issues

The aim of this section is to address the study's second objective, which is to analyse security issues and challenges in adopting cloud-based IaaS. Questions like challenges hindering the adoption of cloud computing in Namibian government, main concerns regarding the use of cloud technology and security concerns as a stumbling block for cloud were addressed.

Respondents were asked to select from a predefined list, the main concerns regarding the use of cloud computing. Majority (98%) of the respondents cited security issues as the main concerns, 75% of the respondents were concerned with privacy issues. Sixty percent feared legal issues and loss of data. It is also evident (36%) that compliance issues, integration issues, insufficient financial benefits and immature technology were less of a concern, with the least worry being lack of functionalities and other concerns (Table 4-5).

**Table 4-5: Main concerns regarding the use of cloud computing**

Respondents (%)	Main concerns	Notes
98%	Security issues	Negative Perception- Main concerns listed are viewed as negative perception towards cloud computing adoption. Below is a scale how this negative perception affects cloud adoption.  ≥ 50%: having a potential effect on the adoption of cloud computing. ≤ 49%: less effect to the adoption of cloud computing.
75%	Privacy issues	
60%	Legal issues	
60%	Loss of data	
36%	Compliance issues	
36%	Integration issues	
36%	Insufficient financial benefits	
36%	Immature technology	
32%	Lack of functionalities	
16%	Lack of performance	
4%	Other	

#### 4.9 Challenges Hindering the Adoption of Cloud Computing by Namibian Government IT Departments

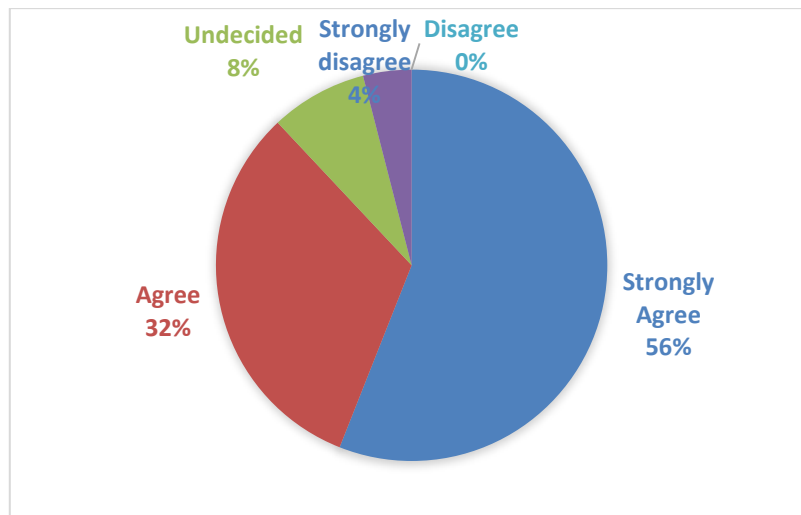
The study results indicate that the majority of the respondents feared the adoption of the technology due to its security and privacy issues (30%) and complexity (23%) of the technology as shown in Table 4-6.

**Table 4-6: Challenges hindering cloud adoption**

Challenges	Respondents	Notes
Security and privacy issues	30%	Negative perception - Challenges hindering cloud adoption by Namibian government IT departments. Below is a scale of how this negative perception affects cloud adoption.  ≥ 50%: having a potential effect on the adoption of cloud computing. ≤ 49%: less effect on the adoption of cloud computing.
Technology complexity	23%	
Unsure of cloud technology	13%	
Cost	13%	
Volume licensing	7%	
Lack of skills to assess and implement	7%	
Legal implications (defining appropriate policies and regulations)	7%	

#### 4.10 Security Concerns as a Stumbling Block for Cloud computing

Respondents were asked if they agreed with the statement: "Security concerns are the blocking issue to cloud computing". The findings reveal that the majority (56%) of the respondents strongly agreed with the statement, suggesting that cloud computing was being hampered by users' perceptions on its security (see Figure 4-7). In addition, 32% of the respondents agreed while 8% of the respondents were undecided. However, 4% of the respondent did not strongly agree with the statement.



**Figure 4-7: Security as a stumbling block to cloud**

#### **4.11 Service Delivery and Accessibility Concerns**

In addition to the perceived challenges affecting the adoption of cloud computing in Namibia, respondents were further asked to list and rate issues affecting IaaS and SaaS service delivery and accessibility. All the respondents cited the availability of the vendor's commitment as the main concerns affecting service delivery and accessibility (Table 4-7). About 96% of the respondents indicated lack of expertise as the second main concern. Other areas of concern regarding service delivery and accessibility include bandwidth and service availability and other minor issues. These issues were perceived as negative perceptions towards cloud adoption, ranked as follows:  $\geq 50\%$ : having a great impact on the adoption of cloud computing and  $\leq 49\%$  having less impact to the adoption of cloud computing.

**Table 4-7: Service delivery and accessibility**

Service delivery and accessibility concerns	Respondents (%) negative impact	Notes
Insufficient vendor service commitment	100%	Negative perception – limited support from the vendors
Lack of expertise	96%	Negative perception – organisations have no experts.
Limited bandwidth capacity	84%	Negative perception – low bandwidth capacity available
Low service availability	44%	Negative perception - down time for service availability

Others	32%	Negative perception: Others include bureaucracy problems and financial support
--------	-----	--

#### 4.12 Interviews

In addition to the online questionnaire survey, face-to-face interviews were conducted to address objective one and two, as well as to propose a secure framework for the adoption of cloud computing technology in Namibia. To ensure equal chance for despondence's participation in the face-to-face survey, each of the 25 respondents were allocated a number on a piece of paper and all papers with respondents' numbers where placed in a container mixed and 13 respondents were identified. Appointments were made with the 13 identified respondents, however only 10 were available for the interviews. Hence, the respondents for face-to-face interviews were identified randomly. Interviews were conducted to address objectives one and two, as well as to validate the components of the framework, which addresses the third and last objective of the study: to propose a secure framework on how the Namibian government can position itself to adopt to the cloud with minimum security risks. The questions for the interview were divided into eight focused categories as indicated in Table 4-8:

**Table 4-8: Interview questions**

Interview questions	Focus
1. Do you think the adoption of cloud infrastructure and software as a service will maximise service delivery in IT and solve backlog problems such as asset underutilisation, hardware failures, lengthy and travel long distance to solve problems and any other IT-related problems?	Maximise service delivery
2. What do you think will be the main cloud challenges in the Namibian IT environment?	Main cloud adoption challenges in Namibian IT environments
3. In Namibia, how would you like your sensitive data to be stored and secured? a. Can we trust cloud providers with the government's sensitive data?	Trust
4. Comparing traditional IT infrastructure to cloud IT infrastructure, what are the security risks?	Security risks



5. Do you believe that cloud computing infrastructure is the future IT model for government despite the security challenges involved?	Cloud computing future IT model
6. What are your recommendation or your input on the Namibian government cloud adoption in the IT department?	Recommendations towards cloud adoption
7. What IT policies and legalisations do you think are critical for Namibian cloud adoption?	IT policies and regulations towards cloud adoption
8. If the Namibian government IT departments consider cloud infrastructure, who should govern it?	Cloud infrastructure governance

This section presents the findings as per the questions.

#### 4.12.1 Maximize Service Delivery

Participants were asked whether the adoption of cloud infrastructure and software as services would maximise service delivery in IT and solve backlog problems such as asset underutilisation, hardware failures, lengthy and long distance travel to solve problems and any other IT related problems.

All participants (100%) were in agreement that cloud infrastructure and software as services would maximise service delivery and solve backlog problems, citing that it comes with the following benefits: service availability, reduce IT infrastructure cost, and provides secure data recovery setup, backup and disaster recovery, ability to solve problems on the click. Hardware failures easily detected, high adoption, applications available everywhere and anytime. No license fees (SaaS subscription based), flexibility and centralised management as recorded in Table 4-9.

**Table 4-9: Maximize service delivery and solve backlog problems**

Will cloud infrastructure and SaaS maximise service delivery and solve backlog problems?	Percentage %	Notes
Yes	100%	<b>Positive Perception:</b> Refers to benefits associated with cloud IaaS and SaaS in maximising service delivery and solve

		backlog problems. Other perceived benefits includes service availability, reduced IT infrastructure cost, secure data recovery setup, backup and disaster recovery, ability to solve problems on the click. Hardware failures easily detected, high adoption, applications available everywhere and anytime. No licence fees (SaaS subscription based), painless upgrades -Public cloud where government can have control over their data -Flexible -centralised management
No	0%	<b>Negative perception:</b> Does not maximise service delivery, unable to solve backlog problems, asset underutilisation, hardware failures, travel long distance to solve IT problems

#### 4.12.2 Main Cloud Challenges

During the interview, participants were asked what they thought would be the main cloud challenges in the Namibia IT environment. The majority of the participants (50%) responded that security would be the main challenge. In addition, 40% of the participants believed that trust was a concern. Furthermore, 30% cited initial budget cost, bandwidth and policies to support cloud as challenges. The least were worried about down time and political interference as indicated Table 4-10.

**Table 4-10: Main cloud adoption challenges in the Namibian IT environment**

Challenges	Percentage %	Notes
Security	50%	No effective security measures in place, cyber attacks
Initial budget/cost	30%	Cost to implement cloud adoption
Trust	40%	-Access by third parties, -Unaware where data is stored -Handing over sensitive data to cloud providers -Data integrity
Bandwidth	30%	-Connections issues. -Bandwidth capacity to support all remote offices, government will spend a lot on the bandwidth connectivity, -No fibre connection in remote areas, -Bandwidth to accommodate all traffic

Policies to support cloud	30%	Lengthy tedious process to draft policies pertaining to cloud
Political interferences	10%	Corruption
Downtime	20%	The ability of the systems/services to be available at all times
Skills	30%	-Namibian cloud expertise

#### 4.12.3 Trust of cloud providers

To obtain participants' opinion on how they could gain the trust of cloud providers, participants were asked to express their perceptions on how they would want their sensitive data to be stored and secured, and whether they could trust cloud providers with the government's sensitive data.

As per Table 4-11, the study found that the majority of the participants (60%) preferred the Namibian government's sensitive data to be stored on a cloud data centre in Namibia. The other 40% believed that Namibian sensitive data should be stored at cloud provider's premises.

**Table 4-11: Where should sensitive data be stored**

<b>Sensitive data storage</b>	<b>Percentage (%)</b>	<b>Notes</b>
Data Centre in Namibia	60%	-Easier to convince decision makers that data is stored in Namibia instead of Europe or elsewhere in the world -Private cloud -Trust team
Cloud providers	40%	-Ensure security since their reputation is at stake -Correct security measures in place

Table 4-12 presents results on whether cloud providers can be entrusted with the government data. The majority (60%) of the participants were positive about entrusting cloud providers with sensitive data. While 40% of the participants refuse to trust cloud providers with the government sensitive data.

**Table 4-12: Can we trust cloud providers with government sensitive data**

<b>Cloud providers trust?</b>	<b>Percentage (%)</b>	<b>Notes</b>
-------------------------------	-----------------------	--------------

Yes	60%	<ul style="list-style-type: none"> <li>-Effective policies and measures in place</li> <li>-Signed agreements/contracts to govern the data</li> <li>-Regulations to control data leakage and data control</li> <li>-Legal framework</li> </ul>
No	40%	<ul style="list-style-type: none"> <li>-Government information can be leaked</li> <li>-Namibia government to govern all their data, in case of password handling etc</li> <li>-Sensitive data to be kept on site and the rest on the cloud</li> </ul>

#### 4.12.4 Security Risks

Comparing traditional IT infrastructure to cloud IT infrastructure, the study reveals that 60% of the participants indicated that cloud infrastructure was more secure than traditional IT infrastructure. However, 10% of the participants feared security issues that come with cloud such as vulnerabilities to third parties/intruders. Traditional IT infrastructure security, as stated by 30% of the participants, involves but is not limited to stolen and faulty hardware, easier access when the passwords are compromised and systems manipulations as shown in Table 4-13.

**Table 4-13: Security Risks**

Security risks	Percentage (%)	Notes: Stated examples
Traditional IT infrastructure security	30%	<ul style="list-style-type: none"> <li>-Hardware can be stolen, hardware faulty</li> <li>-Easier to access</li> <li>-Corruption/system manipulations</li> </ul>
Cloud infrastructure secure	60%	<ul style="list-style-type: none"> <li>-Information is available everywhere</li> <li>-Readily available backups</li> <li>-More secure</li> <li>-Data compromise</li> </ul>
Security	10%	-Vulnerabilities to third parties/intruders

	Traditional IT Infrastructure	Cloud Infrastructure
Comparing traditional IT infrastructure to cloud IT infrastructure, which one is more secure?	<b>30% not secure</b>	<b>60% secure</b> <ul style="list-style-type: none"> <li>-Information is available everywhere</li> </ul>

		-Readily available backups -More secure -Data compromise <b>10% not secure</b>
Security risks	-Hardware can be stolen, hardware faulty -Easier to access -Corruption/system manipulations	-Vulnerabilities to third parties/intruders

#### 4.12.5 Cloud Computing as a Future IT Model

Researchers across the globe believe that cloud computing is the future IT model despite the security challenges (Petrus, Tamm, Stantchev & Ullrich, 2011). Participants were asked their views on the statement: cloud computing Infrastructure is the future IT model for government despite the security challenges involved. Eighty percent of the participants were in agreement with the statement. While 20% said the opposite, as indicated in Table 4-14.

**Table 4-14: Cloud Computing as a Future IT Model**

Is cloud computing the future model?	Percentage (%)	Notes
Yes	80%	-Cloud is the future. -Around the world everything is working towards cloud -Dynamic economic development
No	20%	Cyber war

#### 4.12.6 Future Recommendations for Namibian Government Cloud Adoption

Half of the participants (50%) suggested that the Namibian government should invest in cloud computing investing more on security as seen in Table 4-15 while the other 50% participants recommended that the Namibian government do adequate cloud adoption consultation regarding to understanding cloud adoption, skills and reliable expertise.

**Table 4-15 Recommendations for Namibian government cloud adoption**

Scale	Percentage (%)	Notes
Namibian government should invest in cloud computing	50%	-Cloud infrastructure has many advantages that could benefit the Namibia government -What to roll out on cloud -Well trained community -Proper control over the infrastructure -Committee responsible for the security implementation
Cloud adoption consultation	50%	Understanding cloud adoption and skills -Trust cloud -Agreements to handle data -Reliable expertise

#### 4.12.7 IT Policies and Regulations towards Cloud Adoption in Namibian Government IT Departments

Participants were asked what IT policies and legislations they think were critical for cloud adoption in the Namibian government. According to the study, 50% of the participants suggested cloud governance and cloud security policies, a cyber security policy was also proposed by 40% of the participants and 10% of the participants mentioned IT cloud legislation and management of personal devices and/or laptops as presented in Table 4-16.

**Table 4-16: Suggested cloud IT policies and regulations**

Scale	Percentage (%)	Notes
1- Cyber security policy	40%	
2- Cloud governance policy	50%	Overarching governance policies
3- Cloud security policy	50%	

4- IT cloud legislation	10%	
5- Management of personal devices/laptops	10%	Devices connecting to the government cloud

#### 4.12.8 Cloud Infrastructure Governance in Namibian Government IT Departments

Lastly, participants were asked who should govern the cloud infrastructure should the Namibian government adopt cloud computing. As presented in Table 4-17, the findings show that about 50% of the participants said it should be governed by congress through legislation, followed by cyber security and organisation, which accounted for 40% participants. The least of the participants (20%) believed that it should be governed by a public coalition. None of the participants were in favour of private coalition as shown in Table 4-17.

**Table 4-17: who should govern cloud infrastructure**

Cloud governance in Namibia	Percentage %	Notes
Congress through legislation	50%	Laws to govern
Organisation	40%	Refers to the government IT departments
Public coalition	20%	
Private coalition	0%	
Cyber security	40%	The practice of protecting systems, networks, and programs from digital attacks

#### 4.13 Chapter Summary

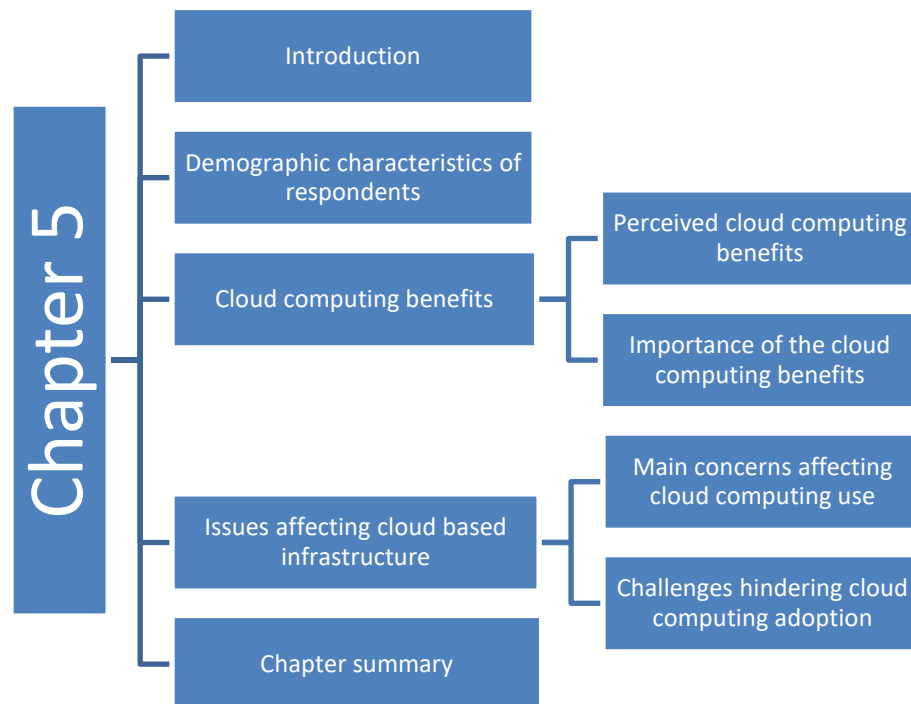
The chapter presented the study as a case study research design and the findings from qualitative data collected through questionnaires, literature review and interviews in an attempt to answer the research questions. The results demonstrated that cloud computing has numerous benefits as a return on investment despite the security risks and challenges. The case study findings are further discussed in the next chapter.

# CHAPTER 5: CASE STUDY FINDINGS, ANALYSIS AND DISCUSSIONS

## 5.1 Introduction

This chapter interprets findings from the results of the previous chapter. The study results were obtained through a self-administered online questionnaire and face-to-face interviews with the Namibian government officials. The findings are presented in five themes, namely: demographic characteristics of the respondents, benefits of cloud computing, security aspects of cloud computing, challenges associated with cloud computing and lastly, the chapter summary.

The chapter map shows the outline followed in this chapter.



## 5.2 Demographic characteristics of the respondents

The respondents in this study, both for the self-administered online questionnaires and face-to-face interviews were purposively stratified from the Namibian government institutions based on the roles of such institutions. The sampled institutions are OPM, MURD and RCs, including decentralised functions. Online questionnaires were forwarded to all IT officials for all institutions, however, 25 out of 30 questionnaires



were answered giving an 83% response rate. Furthermore, the study aimed to verify and acquire additional information from the online questionnaire respondents by interviewing at least half (13) of the respondents, as explained in Section 4.4. Due to non-availability, interviews were only conducted with 10 respondents, which is 40% of the online questionnaire respondents. This was sufficient, as it covered 77% responses of the targeted 100% responses.

The study confirmed that OPM is the leading government agency that approves, oversees and coordinates the implementation of all developmental initiatives within the Namibian government. Hence, the OPM is a key institution in the use of IT infrastructure by the government. Having the OPM implementing cloud computing would put the country at an advantage regarding the use and adoption of cloud computing.

In addition to the OPM, the study also revealed that MURD has a key role to play in the use of IT infrastructure in the government of the Republic of Namibia, as it is responsible for the coordination of the decentralisation of the government functions and houses the RCs. So, in that regard, having MURD using cloud computing will enhance the adoption of cloud computing by the government of Namibia. Like MURD, the RCs will house all the centralised government functions. Hence, the use of cloud computing by RCs and decentralising ministries will advance the government's readiness to adopt cloud. RCs are the implementing agents of government through the decentralisation policy.

As presented in Figure 4-2, the study reveals that most of the respondents were drawn from the RCs due to their active role in the delivery of government services to the citizens. All regional council offices are entrusted with the day-to-day administration functions to ensure the delivery of quality services in the regions. IT infrastructure is key to the success of any office administration, hence, the study of cloud computing was deemed necessary. Most of the other respondents were drawn from OPM and MURD.

The study was conducted on government IT officials at technical and managerial levels, as presented in Figure 4-3. Most of the respondents comprised of the IT system administrators and technicians, as they make up the large number of supportive staff at all levels. In addition, these system administrators and computer technicians are involved in day-to-day IT support activities and hence their views

represent the real-world situations. Other categories such as senior system administrators and technicians as well as the IT managers also play a crucial role in supervising, decision making and soliciting of IT solutions. System analysts and programmers are more involved in IT system specifications and solutions. The use of IT experts in providing information on the adoption of cloud computing can generate reliable information, as asserted by Shimba (2010), who stresses that IT experts' responses confirm the level of reliability of the results and thus provide for good inputs for the design of the framework.

The combinations of various government IT experts in providing information on cloud computing put this study at an advantage as their variety of experiences provide different perspectives of cloud computing understanding. The involvement of these IT experts' portfolios in the use of cloud paradigm enhance knowledge, expertise and confidence on the influence of cloud adoption in the Namibian government.

While it has been presumed that cloud computing was a new concept in Namibia, the study revealed that the majority of the respondents (76%) (Table 4-1) were at least familiar with the cloud computing concept. Of the total respondents, 36% were very familiar with cloud computing, 20% familiar and 20% relatively familiar. This implies that most of the government officials are knowledgeable and fully aware of the cloud computing concept, understand the implications of the cloud technology and are confident to use the technology. However, the study also revealed that 24% of the respondents were just introduced to cloud computing and they were yet to grasp the technology. The study reveals that this high level of understanding cloud computing in the Namibian government put the country in a good position to adopt cloud computing and, hence, to benefit from it. Maluleka (2014) states that knowledge motivates departments to learn more and be willing to adopt cloud computing. Maluleka (2014) further notes that knowledge teaches decision makers how cloud computing works.

Maluleka (2014) says after the orientation and exploration of cloud computing, the users show interest towards cloud computing, search for further information related to costs, benefits and consider cloud as a potential investment for the government. After persuasion, top management considers deciding whether to adopt cloud computing or not. The decision to adopt cloud computing is influenced by benefits/return on investment (ROI), risks and cost.

The study acknowledges and confirms that knowledge or the know-how of new technologies plays an important role in the adoption process. Hence, adapting knowledge as a cloud adoption process.

### **5.3 Benefits of Cloud Computing**

The study analysed the benefits of cloud computing by assessing respondents' perceptions on both the benefits as well as the importance of these benefits. The next sections present an analysis of the perceived benefits.

#### **5.3.1 Perceived cloud computing benefits**

Respondents were asked to express their opinions on what benefits cloud computing delivery services (IaaS and SaaS) have over the current traditional IT infrastructure. Xi and Mitrovic (2014) also confirm that cloud computing has more benefits than traditional IT infrastructure. These benefits of cloud-based infrastructure over traditional IT infrastructure are viewed as positive perceptions because of their positive contribution towards cloud adoption in the Namibian government.

Regarding the perceived benefits of cloud computing over traditional IT infrastructure, 100% of the respondents listed positive benefits of the technology and there were no negative issues associated with the technology. Furthermore, the study reveals that most respondents regarded the technology as cost-effective (Table 5-4), citing that cloud services reduce government cost in terms of infrastructure installations, obsolete hardware and software, consultation fees, maintenance cost and hardware procurement. A fifth of the respondents appreciated the features of centralised resources. Taking into perspective RCs and decentralised function offices in the remote areas, the government will be able to share information centrally among the 14 regions countrywide. Sixteen percent valued the easy accessibility of the paradigm, as the study reveals that cloud services are accessible anywhere if there is Internet access. The study also found that cloud computing addresses the inconvenience caused by the lengthy procurement process currently experienced by the Namibian government, as stipulated in the Procurement Act of 2015. Other cited cloud benefits are maximum hardware utilisation and efficiency. A few respondents appreciated data recovery and backup (8%), improved storage space (8%), IT experts reduced (4%), flexibility (4%) and solved security issues (4%). This is in line with findings from other notable researchers (Kundra, 2011; Services Administration Cloud PMO, 2016; Mohammed et al., 2017; Harfoushi et al., 2016; Alshomrani & Qamar,

2013; Turner, 2013; Trivedi, 2013) that strengthen the benefits of cloud computing and enthuse further that the use of cloud services in government promotes the government institutions to be more efficient, agile and innovative through the effective use of IT investments.

The study also reveals one of the most profound benefits of cloud computing stated by most of the respondents, that is, to “maximise service delivery”. All respondents (100%) were in agreement that cloud IaaS and SaaS will maximise service delivery and solve backlog problems in the IT departments. They indicated that cloud computing comes with the following benefits: “service availability, reduced IT infrastructure cost, and secure data recovery setup, backup and disaster recovery, ability to solve problems on the click. Hardware failures easily detected, high adoption, applications available everywhere and anytime. No licence fees (SaaS subscription based), flexibility and centralised management” as recorded in Table 4-9.

### **5.3.2 Perceived importance of cloud computing benefits**

Cloud computing, particularly IaaS and SaaS, have numerous significance to any government institutions (Mell & Grance, 2009) such as flexibility, cost effectiveness, no upfront payments, IT capacity on demand, increased collaboration, hardware utilisation and centralised IT resources, etc. The study asked the respondents to air their views on the perceived importance of IaaS and SaaS for the Namibian government IT departments. As indicated in Table 4-3, respondents mentioned that IaaS and SaaS were important to Namibian because of the following:

*“Improved service delivery to the public through the use of improved computer resources.”* As well as *“Bringing service closer to the people in a timely manner”*

It was clear from the responses that cloud services improved service delivery. Improved service delivery was an important aspect in the government sector, as the findings indicated that improved service delivery brought more value to the adoption of cloud computing in the Namibian government. One of the participants mentioned that cloud computing “improved service delivery to the public through the use of improved computer resources” and “centralised IT”. Cloud computing enhanced service delivery, as it enabled the dynamic availability of IT applications and infrastructure, regardless of location. This maximised service delivery at OMAs level. The findings also perceived advanced IT infrastructure and availability of information

as important. The respondents revealed that cloud computing saves IT costs. Cloud computing further promises secure backup, and increased performance, increased storage capacity and flexibility. These benefits, shown in Table 4-2, support the findings discussed in Section 4-7 and literature review discussed in Chapter 2.

*“The cost of IT infrastructure is reduced and its uptime is increased. The government will no longer have the responsibility of ensuring uptime, maintaining hardware and networking equipment, or replacing old equipment. IaaS has the ability to scale up and down quickly in response to an enterprise’s requirements. Government has the ability of accelerating the deliverance of product/service to its citizens. Less time is spent on backups and the need to spend on the introduction of new underlying software, time needed to spend on installing/ downloading patches for upgrades or updates. It can keep IT costs consistent or lower than packaged or home-grown software.”*

As much as cloud services can offer uncountable benefits, the study cautions about security concerns including trust associated with cloud computing that needs to be dealt with before adopting cloud computing. Security issues and challenges are discussed later in this chapter. Below are the supporting quotes from the respondents:

*“It will be great, but I am concerned with the security”*

*“It could mean availability of information at all times in terms of portability, security and backups of data made easy. No need to back up or worry if anything happens to your PC/laptop, all its data will be intact. However, there are always security concerns regarding data saved on cloud, especially the GRN data. Issues like confidentiality of data, etc.”*

*“It will be beneficial and eases access to software. Well-supported infrastructure, but it will also mean putting in place IT security measures since it is in government where policy needed to govern how cloud computing is deployed and utilised.”*

The study shows that IaaS and SaaS deploying services primarily mean a lot to the Namibian government IT departments, as demonstrated by the discussed perceived importance of cloud computing services. The respondents’ perceptions were positive and in favour of cloud adoption as well the positive attributes associated with cloud. However, 3% of the respondents were unsure what the technology entailed while about 3% of the respondents had negative perceptions on the importance of cloud computing. The study revealed that these respondents were unsure of the

uncertainties that the cloud technology entails. This could be that they were among those that had just learnt about the technology, as stated in Table 4-1.

In addition to the perceived benefits identified by the respondents, other studies (Mell & Grance, 2009; Kundra, 2011; Alshomrani & Qamar 2013; Turner, 2013; Trivedi, 2013; KPMG, 2010) present up to 15 benefits associated with cloud. The studies suggest that these benefits were the greatest influencers when it came to cloud paradigm adoption. These benefits include increased collaboration, pricing flexibility, no upfront investment, convenience for the development teams, IT efficiency, ability to grow and shrink, IT capacity on demand, new products and services, operational cost savings, software cost savings, hardware utilisation, improved security, better functionality, complexity reduction, better scalability and more flexibility and centralised IT.

This study ranked these benefits in order of importance to OPM, MURD and RCs including decentralised functions. The study found that improved security, hardware utilisation, IT efficiency, IT capacity and demand and better functionality are ranked extremely important. These benefits are of significant importance to the Namibian government IT departments. Namibians look forward to improved security in their systems, especially with the alarming increase in cyber-attacks. Hardware utilisation solves the IT hardware assets underutilisation currently experienced. Efficiency and improved functionalities are strong contributing factors to cloud adoption.

In addition, no upfront investments, better scalability, more flexibility and the ability to launch rapidly are cloud features that are seen as very important to the Namibian government IT infrastructure.

### **5.3.3 Benefits summary**

In conclusion, this section summaries and addresses the first objective of the study, to analyse cloud computing benefits for Namibia's government future IT infrastructure and propose the best approach for adoption. Table 5-1 summaries the best cloud computing benefits for Namibia's government future IT infrastructure.

**Table 5-1: Best Cloud Computing Benefits**

<b>Benefits</b>	<b>Literature reviews</b>	<b>Research findings</b>
Increase collaborations	√	
No upfront investment	√	
IT efficiency	√	√
Growth enabling	√	
IT capacity and demand	√	√
Ability to launch rapidly	√	√
New products and services	√	
Secure backup	√	√
Operational cost saving	√	√
Software cost saving	√	√
Maximise hardware utilisation	√	√
Improved security	√	√
Better functionality	√	
Complexity reduction	√	
Better scalability	√	√
Flexibility	√	√
Improved service delivery	√	√
Advanced IT infrastructure		√
Availability of information		√
Increased performance	√	√
Centralised resources	√	√
Easily accessibility	√	√
Lengthy procurement process solved		√
Data recovery and backups	√	√
Improved storage space		√
IT experts reduced		√

## **5.4 Issues affecting cloud based infrastructure**

This section analyses the main issues affecting the adoption of cloud computing technology in the Namibian government setup. This study identified at least 10 issues and they are grouped into two categories, namely: cloud security and related issues, and challenges hindering cloud computing adoption. The study findings confirm the cloud computing security issues and challenges mentioned in Section 2.6.

### **5.4.1 Cloud security and other related issues**

To analyse the security issues and challenges affecting the adoption of cloud computing in Namibia, the study confirmed, as presented in Table 4-5, the 10 main concerns affecting the security level of cloud computing, as stated and analysed by previous studies (KPMG, 2010). These are security issues, privacy issues, legal issues, loss of data, compliance issues, integration issues, insufficient financial benefits, immature technology, lack of functionalities and lack of performance.

The study also confirmed, with an overwhelming majority of (98%) respondents as shown in Table 4-4, that security issues are the main concern. This is in line with previous studies by Kuyoro et al. (2011) that found that security issues are a big threat to cloud adoption. Additionally, this study rated privacy related issues, fear of legal issues and loss of data as having potential effects on cloud computing adoption in Namibian IT departments.

The study also found that the concerns that were perceived as security issues by over 50% of the respondents had significant effects on the adoption of cloud computing. These concerns related to security issues, privacy issues, legal issues as well as loss of data. Other issues such as compliance, integration, immature technology, lack of functionalities and performance were identified but found to have less effects on the adoption of cloud services.

Comparing traditional IT infrastructure to cloud IT infrastructure, 60% of the respondents stated that cloud infrastructure is more secure than traditional IT infrastructure, adding that appropriate security measures are in place, qualified expertise and more readily available backups. However, 10% of the respondents feared security issues that came with cloud such as vulnerability to third parties/intruders. Traditional IT infrastructure security, as stated by 30% of the respondents, involved but was not limited to stolen and faulty hardware, easier access



when the passwords are compromised and system manipulation, which is shown in Table 5-13.

## **Trust**

The study further reveals that there were mixed feelings among the respondents on whether to trust cloud providers with the Namibian government's sensitive assets and information. The study, in Table 4-11, shows that most (60%) of the respondents preferred the sensitive data to be stored on a cloud data centre where the location was known, preferably in Namibia than elsewhere in the world, as they believed that it was easier to convince decision makers that government data was safely stored where they know rather than by third parties. Forty percent of the respondents believed that data should be stored with cloud providers anywhere, as long as there were correct security measures in place, adding that cloud providers ensure that all security standards are met as their reputation is more at stake.

Regardless of where the data was stored, the study in Table 4-12 shows that more than half of the respondents were positive about trusting cloud providers with sensitive data as long as there were effective policies and measures in place, signed agreements/contracts to govern the data, regulations to control data leakage and data control and legal framework to govern sensitive data. While 40% were hesitant that government information can be leaked and passwords to secure these data can be compromised, they considered other services to be available on cloud and sensitive data on premises.

*“There are security concerns on having sensitive and confidential information saved on cloud, one cannot trust cloud providers.”*

To address these security issues, authors such as Maluleka (2017) and Shaikh and Haider (2011) suggest secure authentication, control of user-access authorisation, confidentiality, compliance and audit, data forensics, transparency and a client-based privacy management tool.

Maluleka (2017) adds that tools such as CloudDataSec are designed for cloud services adhering to government laws and SaaS details the procedure on how to implement security and privacy operations.

#### **5.4.2 Challenges hindering cloud computing adoption**

As experienced elsewhere (Xi & Mitrovic, 2014), the adoption of cloud computing in Namibia is also not free from the cloud paradigm technological challenges.

The results indicate that most of the respondents feared the adoption of the technology due to its security and privacy issues (30%) and complexity (23%) of the technology (Table 4-6). Regarding security and privacy issues, respondents raised concerns such as unnecessary loss of data, accessibility of confidential data by third parties and the challenge of trusting an unknown institution to manage the government's valuable data. This was in line with findings by other authors such as Sen (2013), Brodtkin (2008) and Hashemi et al. (2013).

In terms of technology complexity, the respondents were unsure of the availability of the network bandwidth and poor unsupported network infrastructure, especially in the remote areas such as the RCs. Even though complexity issues have been cited by other authors in relation to the readiness to adopt cloud, authors such as Xi and Mitrovic (2014) found this challenge to be less important, as the availability of Internet technology has improved significantly across the globe. Namibia has one of the best Internet infrastructures provided by West Africa Cable System (WACS) optic fibre cables that link Africa to Europe. However, the status of localised Internet infrastructure may be affected by budget constraints. For instance, the need to improve the Internet bandwidth, especially in the regions, is affected by the Namibian government's limited budget. Other challenges listed by respondents include fear of investment cost, limited IT (cloud) knowledge, volume licensing as well as the legal implications such as cloud security policies.

In addition to the security concerns, the study revealed that the adoption of cloud computing in the government of Namibia was anticipated to be hindered by various challenges some of which are related to security, technological and financial constraints, licensing and skills. In general, all the identified challenges appear to have less effect on adoption of cloud computing in the Namibian government. Of these security and privacy issues related to cloud services, activities were found to be main (30%) challenges that could potentially hinder the Namibian government from adopting cloud computing. The technology complexity and uncertainty of cloud technology were the second main challenges associated with the adoption of cloud based services. Others included volume licensing and skills. However, their effect

appears to be minimal, as shown in Table 4-6. To highlight the significance of the security concerns among the government IT officials, the study found that 56% of the respondents were strongly supporting the notion that security concerns were stumbling block to the adoption of cloud computing. As shown in Figure 4-8, this might be contributed by cloud computing familiarisation and alarming cyber war, one should think twice before migrating to cloud. The findings confirm that security has a significant negative effect to the adoption.

*“Bandwidth, cost and network coverage”*

The challenges associated with cloud computing were mainly related to factors affecting cloud services delivery and accessibility. About 100% of the respondents feared the unavailability or insufficient commitment by the vendors. Furthermore, 96% and 84% were concerned about lack of expertise and limited bandwidth capacity, respectively. Table 5-7 shows that these three factors were found to have the potential to slow the adoption of cloud computing by the Namibian government. Other factors such as downtime for service availability, bandwidth, bureaucracy and financial support were found to have less effect.

Furthermore, the interviews also confirmed that security is the main challenge, as there are currently no effective cloud security measures in place and with the alarming cyber-attacks, security is one of the greatest concerns. In addition, 40% of the respondents believed that trust is a concern. Trust comprises data accessed by third parties, unaware where data is stored, data integrity and handing over sensitive data to cloud providers. The study further found that the initial budget cost to setup the cloud infrastructure, bandwidth and policies to support cloud were some of the challenges indicated. 20% of the respondents were worried about downtime and 10% of the respondents were worried about political interferences, as reflected in Table 4-10.

*“We have no IT development frameworks of our own and no IT policy to control and regulate the utilisation of the cloud, or IaaS nor SaaS as far as cloud computing is concern”*

The study revealed that most of the participants were more concerned about legal aspects, such as policies and regulations, concerning cloud computing. The interview results confirmed that policies and regulations are very critical to the adoption of cloud

computing in the Namibian government. Mell and Grance (2011) state that standards and guidelines provide adequate information security for all the government's operations and assets, also at national level. The study found cyber security, cloud governance policy, IT cloud legislation, cloud implementation guidelines, cloud computing policy, technology integration policy, cloud security alliance, government audit and management of personal devices as critical policies needed for the adoption of cloud computing in the Namibian government. Furthermore, Mell and Grance (2011) suggest that cloud infrastructure should be governed through congress legislation, organisation and cyber security.

The findings of this study confirm with the statement that "cloud computing infrastructure is the future IT model for government despite the security challenges involved", as shown in Table 4-14.

## **5.5 Factors influencing cloud computing adoption**

The issues affecting the adoption of computing were broadly divided into four categories, namely: organisational factors, technological enablers, environmental factors and users/stakeholder characteristics.

### **5.5.1 Organisational factors**

The organisational factors are factors that are influenced by the organisational characteristics and management. In this context, the Namibian government IT technology is governed by OPM that, among others, is responsible for setting up legislation and policies for the procurement and use of cloud computing infrastructure. At ministerial and sub-national level (RCs), the use of cloud infrastructure is managed by the top management and IT experts. However, the study reveals that there is a need to capacitate the government IT officials. The other option of dealing with government's capacity to use cloud computing technology would be to have reliable service providers and other role players meet government half way. The study presents the sub-factors within the organisation that affect the adoption of cloud computing:

#### **5.5.1.1 Needs Assessment**

The study has revealed that there is a need for the Namibian government IT departments to carry out a departmental needs assessment to determine the needs and expectations of the government. This is to ensure that the cloud computing innovation meets and addresses the needs and expectations of the departmental objectives. This helps to determine the organisation's operational readiness and strategic consideration, as it includes assessing the department's IT infrastructure and requirements for the organisation's sustainability. The study further indicates the need to evaluate the government's internal competency skills, management support, infrastructure availability and resources for the adoption.

#### **5.5.1.2 Benefits**

This element refers to the perceived value that cloud computing will add to the Namibian government should it invest in cloud technology. The study revealed that cloud computing could maximise service delivery, reduce cost, increase performance, eliminate lengthy procurement processes, increase effectiveness, centralised resources, enhanced information availability, flexibility, disaster recovery, improved storage space, reduction in IT complexities, reduction in number of IT experts, systems integration, software legacy, auditing, environmental friendliness and the ability to launch rapidly, which is a great return on investment to the Namibian government.

#### **5.5.1.3 Executive management buy-in**

The study found that top management support is very important to the implementation of cloud adoption. The executive management should understand and grasp the value of the technology to advance and inform their decision-making strategies. The study revealed that there might be some political influence that might impact the decision, however, once the executive management supports the initiative, it is likely to be approved and implemented.

*“Less knowledge from decision makers and having older persons in the lead, and the older appreciate technology less than younger generations.”*

#### **5.5.1.4 Budget**

As discussed in Chapter 2, and in the study findings, the study revealed that cloud computing is a cost-effective technology and is good value for money. However, the respondents believed that when implementing cloud adoption an initial budget is needed, and that the benefits should outweigh the budget costs. The budget might include the feasibility study cost, initial cloud computing acquisition budget and service-level agreement cost.

#### **5.5.1.5 Information security**

The study shows that security is a serious concern in cloud adoption. This factor assesses the risks associated with data security and privacy. At organisational level, the study recommends these security controls: trust management, confidentiality, transparency, accountability and privacy.

#### **5.5.1.6 Governance**

The study recommends governance as an important factor in the implementation of new technologies. Governance entails the set of responsibilities and practices by executing management in providing strategic direction and ensuring that objectives are met. According to ISACA (2011), when adopting cloud service, all business processes are compacted. Furthermore, for the government to benefit from cloud computing usage, “a clear governance strategy and management plan must be developed”. The strategy sets out the directions and objectives for the adoption of cloud-based services in the Namibian government. The management plan aims to execute the objectives.

The following are ensured and met through governance:

- Strategic alignment of IT infrastructure to the organisation’s mission, needs and goals;
- Value delivery: ensuring that the cloud adoption strategy delivers benefits and provides value;
- Resources management: the availability and management of adequate resources
- Measurement of IT department performance to monitor progress towards cloud adoption

- Compliance of IT cloud legislation and policies
- Identifying controls to mitigate known risks
- Provision of support for efficiencies and continuous improvement
- Transparency in decision making
- Understanding and awareness of cloud computing risks, and effective and appropriate management of these risks.
- Stakeholders trust the government's strategy
- Service monitoring and auditing (Shimba, 2010)

#### **5.5.1.7 Skills**

Skills shortage was another concern the respondents stated. The study revealed that more cloud expertise is needed in the Namibian government to run the cloud infrastructure, as none of them have experience. Skills are an important element in the adoption process. The organisation's competency determines what the department lacks and what will be sourced from cloud providers.

#### **5.5.1.8 Performance**

The study found that cloud infrastructure performance influences the decision of the decision makers. The performance indicators of cloud adoption include compliance, scalability, reliability and the availability of services offered.

### **5.5.2 Technological enablers**

The organisational factors are those factors that enable and promote cloud computing technology. These factor determine the technological needs of the government by means of internal and external technologies. Awa et al. (2015) argue that the successful adoption of IT depends on the technology competence of the organisation.

#### **5.5.2.1 Infrastructure readiness**

The study found three infrastructural readiness indicators namely: electricity availability, reliability and bandwidth.

The study found that it was very important to have electricity that is reliable and available always, especially in all 14 regions countrywide, as unstable electricity

supply hinders service reliability and limits service accessibility. A fast and reliable Internet access across the entire country is considered essential for cloud adoption. However, the study found concerns with the slow bandwidth experienced in the regions. Respondents complained about slow Internet access in some remote areas. The study recommends that the government invest in bandwidth upgrade nationwide.

#### **5.5.2.2 Compatibility**

Compatibility is the degree to which cloud computing fits with the existing systems and applications. The study found out that when the technology is recognised as compatible with work application systems, organisations are likely to consider adopting cloud computing.

#### **5.5.2.3 Security and privacy**

The study shows that security is a serious concern in cloud adoption. This factor assesses the risks associated with data security and privacy. At technology level, the study recommends these security controls: trust management, confidentiality, transparency, accountability, identification and authentication management, authorisation and access control, integrity, non-repudiation, network security, governance, data centre physical security, privacy, and monitoring and evaluation.

#### **5.5.2.4 Challenges**

The study recommends that before adopting cloud technology, government should address all challenges mentioned in section 5.4.2.

#### **5.5.2.5 Service delivery**

The study found service delivery as important to cloud adoption in the Namibian government. The innovation could maximise service delivery in all Namibian government IT departments as well as the citizens.



### **5.5.3 Environmental factors**

This factor deals with the environment in which the organisation operates. This includes policies, regulations, service providers, and governance and information technology. Cloud adoption promotes a competitive environment by industry structures and outperforms other organisations with overwhelming cloud benefits. The main benefits organisations are expected to derive from cloud computing are competitive advantage and survival (Gangwar et al., 2015).

#### **5.5.3.1 Policies and regulations**

The study identifies the compliance of policies and regulations as a necessity for cloud adoption. The findings suggest proper policies and regulations to be crafted for the Namibian government. The study recommends the following policies: cyber security policy, cloud governance policy, IT cloud legislation, cloud implementation guidelines, cloud computing policy, technology integration policy, cloud security alliance and government audit.

#### **5.5.3.2 Service providers**

Organisations rely on cloud service providers' experience, skills and the ability to deliver or to make services available when needed. Security and accountability of the service providers plays an important role. Service provider scarcity refers to the lack of reputable and qualified cloud service vendors in the cloud service market in Namibia. The availability of enough vendors with a good reputation improves the organisation's confidence in cloud services. According to Li et al. (2015), vendor scarcity has a negative influence on an organisation's trust towards cloud computing adoption. The study confirmed that all SLA considerations should be covered to differentiate expectations from the cloud service providers.

#### **5.5.3.3 Information security**

The study shows that security is a serious concern in cloud adoption. This factor assesses the information security risks associated with the operational environment. The study stresses that when adopting cloud computing the government has to ensure that the technology complies with all the standards and procedures. Secondly, to ensure that all procedures are governed in accordance with the government's strategic plan. Thirdly, trust and privacy have to be maintained. Lastly, the service

provider has to ensure that the data centre physical security is not compromised at any cost.

#### **5.5.4 Users' characteristics**

The users' characteristics factor includes the characteristics and roles of all stakeholders involved in executing the framework in the Namibian government IT departments.

##### **5.5.4.1 Awareness, knowledge and skills**

The study revealed that the awareness of cloud computing is very important to all users. Mahlindayu, Bakhtiar and Rusli (2014) perceive that lack of awareness and knowledge on cloud computing had hampered governments from embracing the full potential offered by the technology. The findings encourage the service providers and the government to formulate strategies to promote the use of cloud computing in government. All users must be educated to fully utilise and enhance cloud computing technology.

To fully acquaint themselves with the necessary cloud computing skills and knowledge, users have to understand the process and be well informed. This helps in making well-informed decisions by the executive management and maximum utilisation of technology. The right skills and knowledge experts are needed for the implementation of cloud adoption. The management within the Namibian government becomes aware and knowledgeable about cloud computing technology and its functionalities. The IT departments are persuaded and perform needs analysis assessment on the technological, environmental and the competence of the organisational context factors based on the departmental requirements.

##### **5.5.4.2 Acceptance**

This phase examines the extent to which the government believes that cloud technology is useful and easy to use. This is the crucial stage for users to access the cloud services deployed. This ensures that the cloud services to be accessed are available and that all security and privacy requirements are implemented. For users to trust accessing the cloud services (technology), the following security controls

should be in place: confidentiality, availability and integrity of data or information, authentication, authorisation, access control, transparency and compliance.

The study encourages the Namibian government to invest in cloud infrastructure because of its numerous benefits. However, it recommends proper cloud adoption consultation prior to adoption to determine the skills capacity and to develop more understanding on trust and reliability.

## 5.6 Chapter summary

This section summarises the findings of the study and further addresses the objectives of the study by answering the study questions.

**OBJECTIVE 1: To analyse the cloud computing benefits for Namibia's government future IT infrastructure and propose the best approach for adoption.**

According to the study analysis, Table 5-2 summaries the best cloud computing benefits for Namibia's government future IT infrastructure.

**Table 5-2: Best Cloud Computing Benefits**

Benefits
Flexibility
Centralised resources
Hardware utilisation
Scalability of IT resources
Greater IT efficiency and agility
Cost reduction
Increased performance and better functionality
Rapid elasticity
Protection, care and technical support
Auditing and logging
Reporting and intelligently
Policy management
Systems integration and software legacy
Business continuity
Regular backup and disaster recovery
Maximise improved service delivery
Accessibility of services

Improved storage space
Lengthy procurement process eliminated
IT experts reduced
Improved security
Enhanced availability of information
Environmental friendly
Reduction in IT complexities
Ability to launch rapidly

**OBJECTIVE 2: To analyse security issues and challenges affecting the adoption of cloud- based Infrastructure as a Service in Namibia’s government institutions and propose secure solutions.**

**Table 5-3: Security Issues and Challenges Affecting Cloud Computing**

Security issues/Challenges	Solutions
Security issues	Ensures network security, identity and access management, authentication and authorisation, confidentiality, integrity, availability, monitoring and incident response, policy management and privacy
Privacy issues	Confidentiality and privacy management tools
Technology complexity	Select skilful and experienced service providers, who have implemented the technology before.
Trust of where government data stored	Confidentiality, non-repudiation, identification and authentication management, auditing, monitoring and evaluation, transparency, authorisation and access controls
Data integrity	Ensures integrity, transparency
Political interferences	Compliances, auditing, monitoring and evaluation
Compliance issues	Governance and enforcement of the policies
Lack of performance/functionalities	Accountability Train IT experts
Lack of skills to assess and implement	Awareness and knowledge capacitate Request training from service providers
Integration issues	Perform a needs assessment and draft a technology integration policy in consultation with the service provider
Inadequate IT budget for volume licensing	Implement cloud computing in phases
Legal implications	Governance

Insufficient vendor service commitment/lack of expertise	Sign service level agreements clearly stating the commitments between the two parties
Limited bandwidth capacity	Upgrade bandwidth capacities in the
Low service availability (downtime)	Maximise uptime, prioritise network traffic
Initial cost/budget	The government should strategies, budget and avail funds
Trust	Trust management tool
Policies to support cloud	Draft cloud security policy, cloud governance policy, cloud implementation guidelines, Technology integration policy and create cloud security alliance
Cloud infrastructure security	Ensures accountability, data centre physical security, Access control and authorisation

***OBJECTIVE 3: To assess the Namibian government IT departments readiness to adopt cloud computing.***

The study concluded that the majority of the Namibian government IT officials are aware of cloud computing. The cloud computing paradigm offers incredible benefits such as scalability, increase productivity and efficiency. The respondents show great positivity towards the cloud adoption readiness in Namibian government IT departments as reflected in the results section. This is the first and important milestone towards addressing the challenges faced by the Namibian government IT departments. However, while acknowledging the technology's advancement gains, the study indicates that more still needs to be done on the challenges and concerns. Security and privacy issues play an important role in hindering the adoption of cloud service in many instances. In this study the findings reflect that most respondents fear trusting Namibia's data and information with a third party. Technology complexity, lack of skills and cloud computing uncertainties are also factors challenging the readiness. Legal frameworks such as cloud security policy and cloud adoption strategy still need to be developed.

***OBJECTIVE 4: To propose a secure framework on how the Namibian government can position itself to adopt cloud computing with minimum security risks.***

The study shows that around the world, many countries have successfully adopted and some are considering the adoption of cloud computing technologies in their governmental offices. With studies emerging around the globe of cloud adoption

readiness and cloud adoption frameworks in the public sector, the secure framework proposed by this study in the Namibian government is redeemed relevant and beneficial.

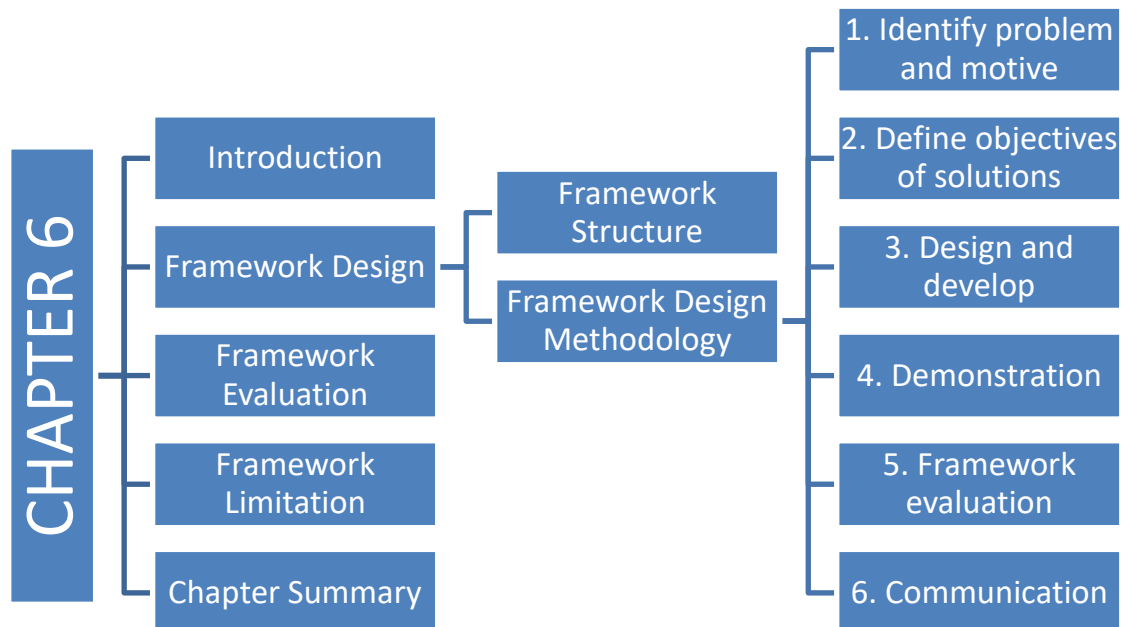
The study gathered factors that will enable cloud adoption in the Namibian government and these factors are crucial in the development of the framework. These factors are grouped into four categories, namely: technological enablers, organisational factors, environment factors and stakeholder characteristics. The framework design is discussed in the next chapter.

# CHAPTER 6: FRAMEWORK DESIGN PROCESS

## 6.1 Introduction

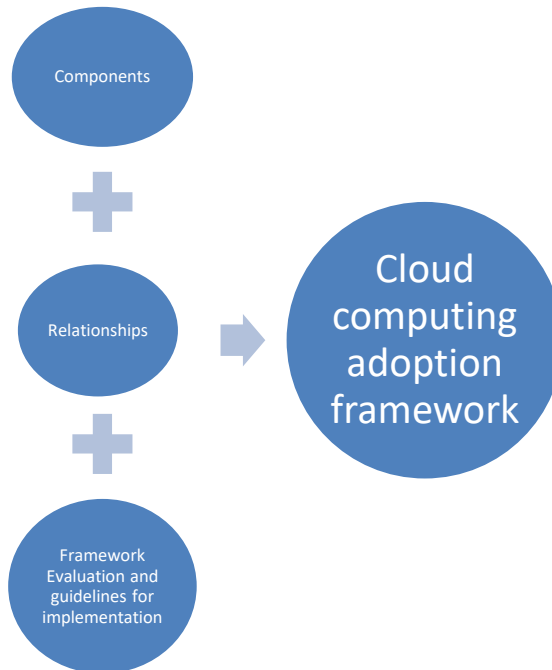
This chapter presents the process that was used to develop the framework using the DSR method by Hevner (2007). The DSR methodological design process for the framework is presented with the following phases: phase 1 identifies the problem; phase 2 defines the objectives of the solution, and phase 3 presents the design and development of the framework. Phase 4 demonstrates the actual framework. Phase 5 evaluates the framework and finally phase 6 communicates the framework.

The map below presents the outline of the chapter.



## 6.2 Framework design

According to von Roessing (2010), a framework gives a detailed structural description of how to implement, create or manage a programme or process. This study details the description of the framework structure designed by identifying the framework components, and applying the definitions and existing knowledge. Figure 6-1 presents the framework structure.



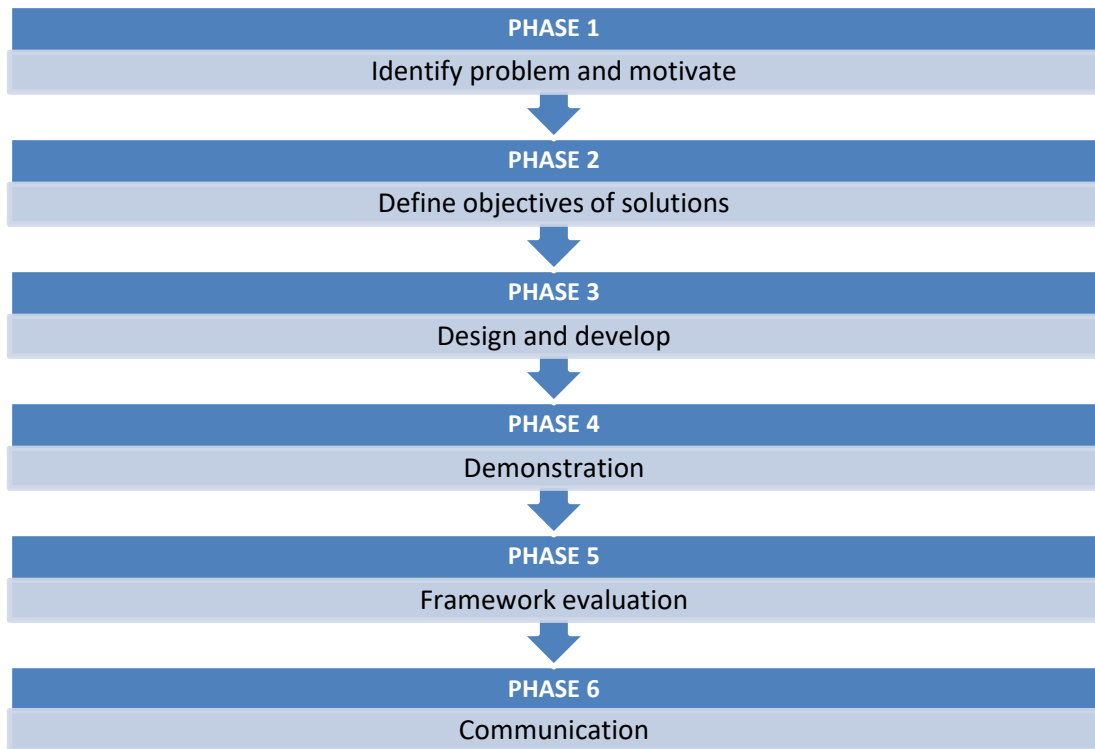
**Figure 6-1: Framework Structure**

### 6.2.1 Framework Design Methodology

This section presents the framework design methodology process based on the literature review, problem identification and DSR method. For the success of this framework design, the study adopted the DSR design elements by Hevner et al. (2007). The component identification was done in Section 5.5.

Figure 6-2 summarises the application of DSR framework design process in phases:





**Figure 6-2: Framework Design Process (Source: Hevner et al., 2004)**

### **6.2.2 PHASE 1: Identify problem and motivate**

The framework development was motivated by the research question: “In what ways can the Namibian government position itself to adapt to the cloud-based service with minimum security risks?”

To further scrutinise and answer the question, two other questions were asked as follows: “what benefits does cloud computing yield to Namibia’s government future IT infrastructure?” and “what are the security issues and challenges in adopting cloud-based IaaS in Namibian government institutions?” The study findings in Chapter 2, 4 and 5 answered these questions with the following problem identification and motivation:

**While traditional IT infrastructure faces low server utilisation, fragmented demand, expensive to maintain and systems that are difficult to manage, cloud computing has the potential to improve government service delivery, reduce operating costs, increase data centre efficiency and server utilisation. The study investigates the benefits and challenges associated with cloud-based**

infrastructure services and proposes a secure framework to adopt cloud computing in the Namibian government IT departments.

Figure 6-3 summarises problems faced by the Namibian government.



**Figure 6-3: Problems faced by the Namibian government IT departments**

The objective and motivation of this phase is **“to propose a secure framework for cloud adoption in the Namibian government IT departments”**.

### **6.2.3 PHASE 2: Define objectives of solutions**

According to Hevner and Chatterjee (2010), problem relevance stipulates the objectives of the research to develop the solution to the organisation's problems. Peffers et al. (2007) add that at this stage the study defines the objectives of the solution from the problem definition.

The main objective:

**The aim of this study is to assess and investigate the benefits and challenges associated with adopting a cloud-based Infrastructure service, readiness to**

**adopt cloud computing and propose a framework for secure cloud adoption in the Namibian government IT departments.**

Specific objectives:

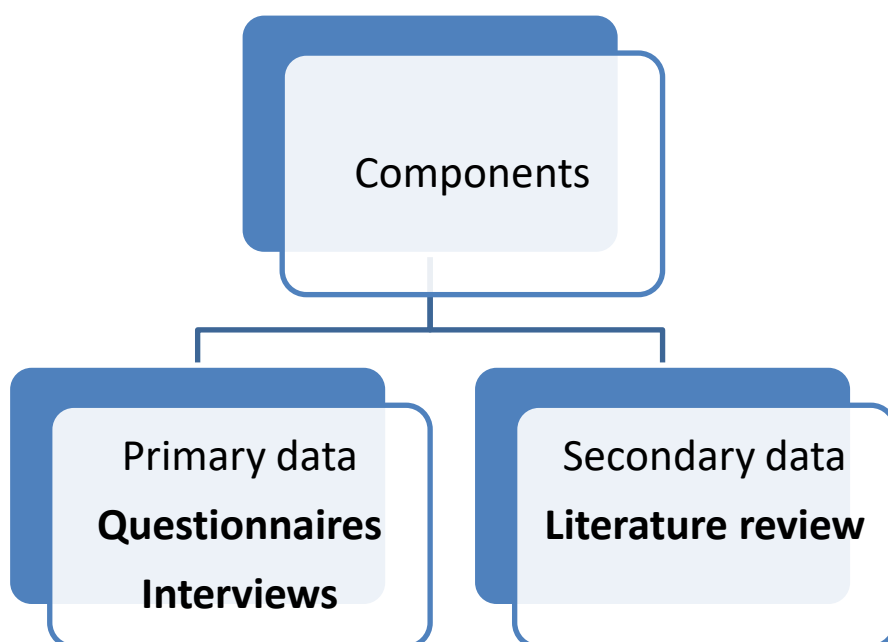
- To analyse the cloud computing benefits for Namibia's government IT infrastructure and propose the best approach for adoption.
- To analyse security issues and challenges in adopting cloud based IaaS in Namibia's government institutions and propose secure solutions.
- To assess the Namibian government IT departments' readiness to adopt cloud computing.
- To propose a secure framework on how Namibian government can position itself to adopt to the cloud with minimum security risks.

#### **6.2.4 PHASE 3: Design and develop**

This section, based on the study findings in section 5.5, details the framework of the identified components and the evaluation of these components.

##### **6.2.4.1 Components identification**

The components were identified from the primary and secondary data sources as illustrated in Figure 6-4.



**Figure 6-4: Components Identified from Data Sources**

The research findings were extracted from the analysis of questionnaire and interview data. The study valued the findings, as the participants' responses are very important sources of theory (Mpekoa, 2017). These theories are real phenomena and inform of the participants' actions, actual beliefs, values and theories (Maxwell, 2012; Hughes, 2007; Charmaz & Belgrave, 2002). The participants have experience with the technology being studied and have more insight than the researcher (Mpekoa, 2017), hence, their opinions play a critical role in designing relevant solutions for their environment.

Existing theories and relevant research facilitate the understanding of the technology being studied.

The study has come up with a concise list of components identified that are crucial to the framework in for the Namibian government to embrace cloud computing. The identified components from literature review and research findings were integrated and grouped according to the four TOE framework focus areas namely: technological enablers; organisational factors; environmental factors; stakeholder characteristics, as shown in Table 6-1

**Table 6-1: Identified Framework Components**

<b>Components</b>	<b>Sub-components</b>	<b>Section</b>
<b>Organisational factors</b>	Budget	Section 5.5.1.4
	Needs assessment	Section 5.5.1.1
	User characteristics	Section 5.5.4
	Executive management buy-in	Section 5.5.1.3
	ROI (benefits)	Section 5.5.1.2
	Trust and privacy (information security)	Section 5.5.1.5
	Governance	Section 5.5.1.6
<b>Technological enablers</b>	Infrastructure readiness	Section 5.5.2.1
	Compatibility	Section 5.5.2.2
	Performance	Section 5.5.1.8
	Information security	Section 5.5.2.3/4
	Service delivery	Section 5.5.2.5
	Privacy	Section 5.5.2.3
<b>Environmental</b>	Policies	Section 5.5.3.1
	Regulations (cloud, trust and privacy)	Section 5.5.3.1
	Governance	Section 5.5.3.3
	Cloud providers	Section 5.5.3.2

<b>User/stakeholder characteristics</b>	Acceptance	Section 5.5.4.2
	Awareness and knowledge	Section 5.5.4.1
	Decision making	Section 5.5.4.1
	Expectations	Section 5.5.4.1
	Information security (trust)	Section 5.5.3.4
	Skills	Section 5.5.1.7
	Motivation	Section 5.5.1.4.

Furthermore, the identified components were clustered according to the adoption process explained in the next section of component validation.

#### **6.2.4.2 Component validation**

Component validation describes the validation of each of the constructs used during the development of the framework. Findings in Chapter 4 and literature review in Chapter 2 validated the constructed framework. Four steps involved in the cloud computing adoption process were identified, namely the technological availability, awareness, knowledge and skills and lastly the decision making in section 2.8.1.5, according to Kaisler et al. (2012). On the other hand, the study adopted Tomatzky and Fleischer's Technological Organizational Environmental framework as presented by Harfoushi et al. (2016). The next section describes the adoption process in the SCAF framework.

- **Technological Availability**

The adoption process starts with the availability of the cloud computing technology in the organisation and, for this study, in government departments. However, the availability of cloud computing technology is influenced by organisational factors; technological factors; environmental as well as technological users' characteristics. Organisational factors affecting technological availability include resource availability such budgetary provision and governance of such resources in favour of the cloud computing technology, as found in section 5.5.1. Technological factors are infrastructure compatibility, bandwidth and challenges, as presented in section 5.5.2. Environmental factors are policies, regulations and cloud providers, as presented in section 5.5.3. Technological user characteristics are presented in section 5.5.4, which include technology acceptance by the users.

Furthermore, the availability of technology is influenced by enabling technological infrastructure that is capable of delivering the necessary cloud services. The study revealed that all sampled government institutions were well equipped with information technology compatible with cloud service provision, as reported in section 5.5.2. The next section presents the awareness of the adoption process:

- **Awareness**

Awareness is very important in all aspects affecting cloud computing. For the executive management to buy in and make well-informed decisions, they should be aware of the technology and decide if its benefits are worth investing in for the Namibian government. The study shows that IT experts are aware of cloud in Section 5.5.4. Knowing the technology, is also important to study the environment in which cloud operates. By assessing the policies, regulations, service providers, security controls and ensuring that the expectations are met. Organisational factors that are at awareness level are executive management buy-in and benefits presented in Section 5.5.1. Technological enablers ensure that security and privacy requirements and controls are known as presented in Section 5.5.2.3. Environmental factors ensure that policies and regulations are also known as presented in Section 5.5.3. Lastly, user characteristics are presented in section 5.5.4.1 and include awareness and expectations. The next section presents the next adoption process.

- **Knowledge and Skills**

Knowledge and skills are power in adopting cloud. The executing management should know and understand the whole process of cloud adoption to lead and approve the project. This element involves using the skills and knowledge to define proper policies and regulations governing cloud computing. Governance should be practised. ISACA (2011) defines governance as a set of responsibilities and practices exercised by management to provide strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed properly. As reported in Section 5.5.4 and evident in Figure 6-10. The next section discusses the decision making of the cloud adoption process.

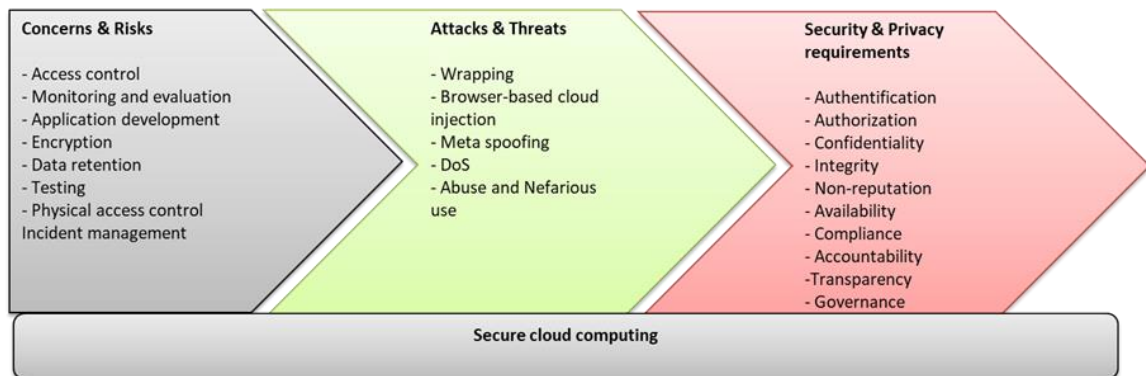
- **Decision Making**

The study reveals in Section 5.5.1 that based on the adoption factors, the decision to adopt cloud paradigm is influenced by the performance or whether the system is delivering service as expected. Security and Privacy plays an important role on the sensitivity of data and infrastructural protection. The overall decision is made on trust

regarding all aspects of cloud adoption. The components of the decision making at the different adopting factors are shown in Figure 6-10. The next section presented is the security and privacy requirements.

- **Security and privacy**

These elements assess the risks associated with security, privacy and other threats and ensures that security measures are in place as shown in Figure 6-5.



**Figure 6-5: Security Mitigations**

The next section presents the monitoring and evaluation of the adoption process.

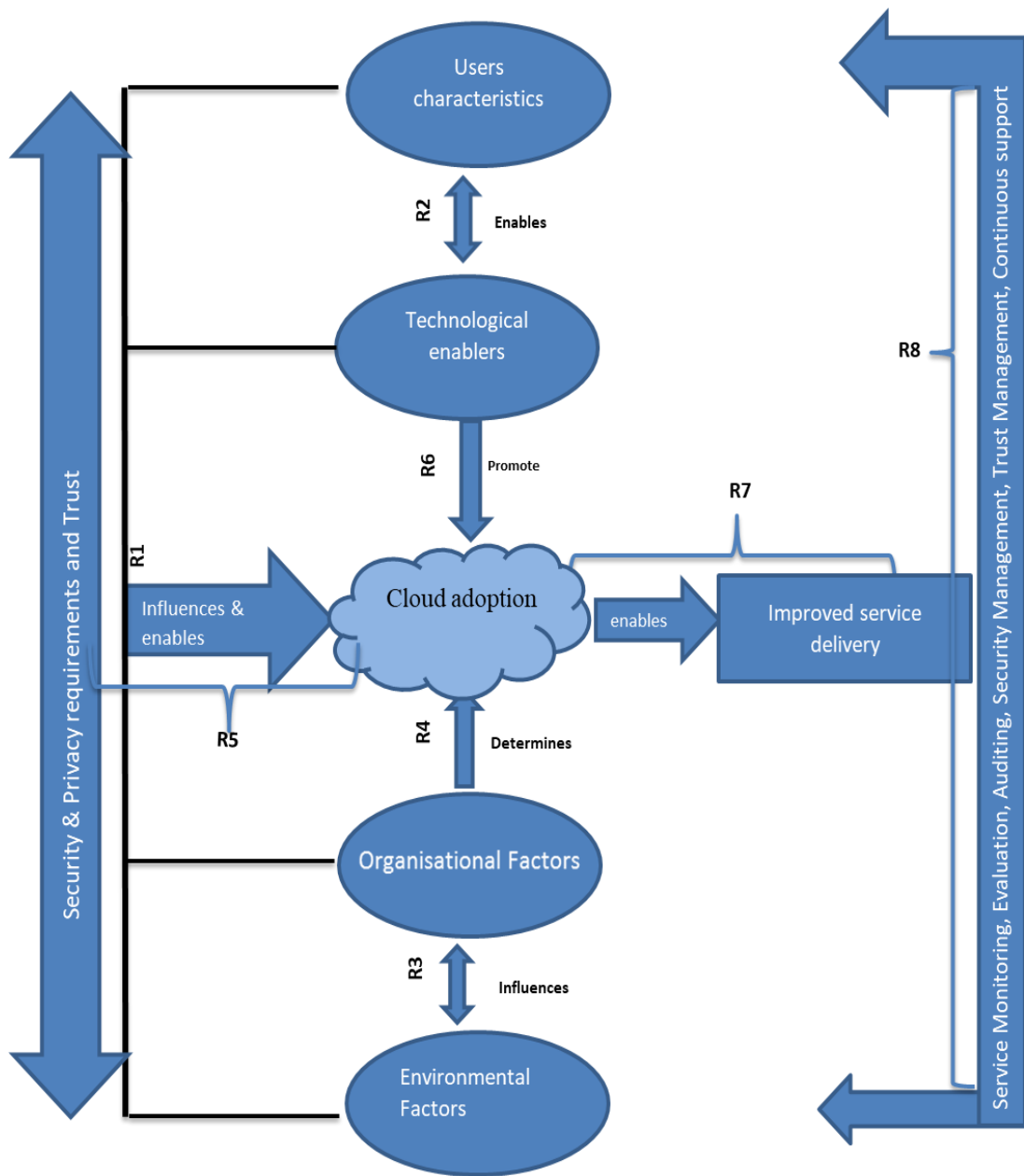
### **Monitoring, Evaluation, Auditing and continuous support**

Knowledge and skills ensures sustainability of cloud adoption, executive management must provide continuous support throughout to drive the implementation of cloud technology. Performance monitoring, evaluation and auditing must be performed constantly to detect any risk or threats that might occur as stated in the study outcomes. This is presented in figure 6-10. The next section presents the construct of the relationships.

#### **6.2.4.3 Construct Relationship**

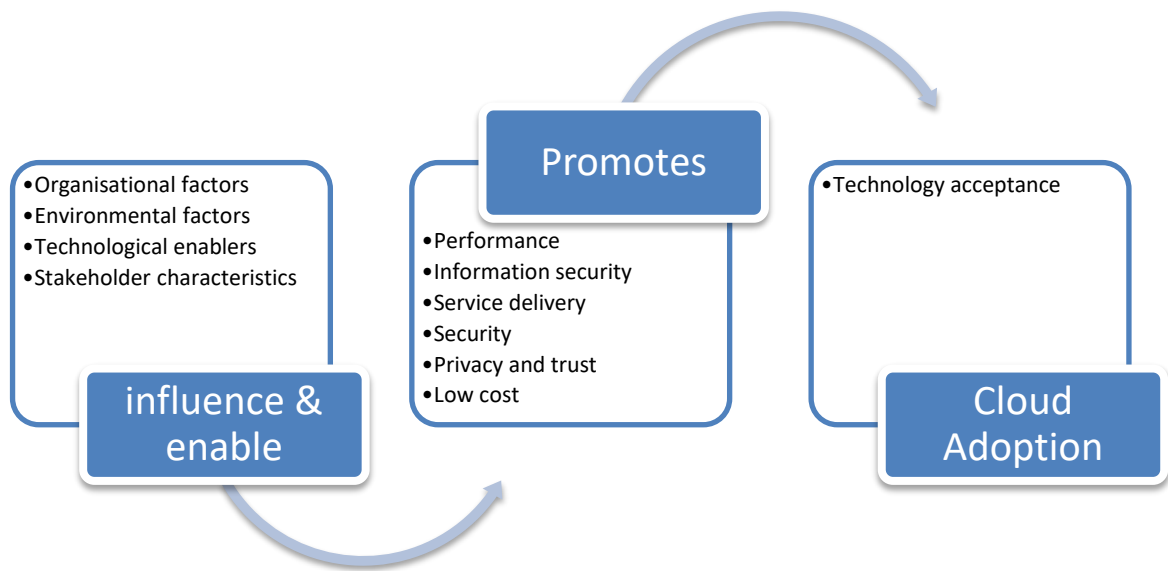
This section presents the relationship of all the constructs involved in developing the framework. Figure 6-6 summarises the interrelationships among the constructs.





**Figure 6-6: Construct Overall Interrelationships**

**Relationship 1:** The first relationship identified is the relationship between the **users' characteristics, technological enablers, organisational factors and environmental factors**. These four components influence and enable the decisions to adopt cloud computing technology. Figure 6-7 shows how this relationship promotes cloud adoption by ensuring that the cloud technology performs, delivery services, lows cost, ensures governmental privacy, trust and to make sure that security (including information security) is always achieved.



**Figure 6-7: Components Relationship**

**Relationship 2:** The second relationship is between the **user characteristics and technological enablers**. Users play an important role in influencing any technological initiatives. Based on the new technology available, the organisation identifies and assesses organisational needs. The executive management are aware and understand the return on investments (benefits) of cloud-based technology to the business strategy. Once the departmental objectives and expectations are achieved, the technological readiness is assessed. The overall infrastructure is assessed if the technology is compatible with the current infrastructure and if the Internet bandwidth will be able to accommodate all users, and data security and privacy measures are considered. Based on trust, performance and service delivery, the executive management buys into the technology's adoption.

**Relationship 3:** The third relationship is between **environmental factors and organisational factors**. Governance: the cloud infrastructure requires well defined policies and regulations. And implementing within an organisation with well-defined roles of responsibilities of IT management, business processes and applications helps the organisation to address the areas of regulatory compliances, risk management and align IT strategy with organisational goals. The study promotes the implementation of controls

where legal requirements, legislation, policies and standards can effectively protect the data. Controls such as cloud preventive controls, which include risk analysis and decision support tools, enforcement of policies and trust management.

**Relationship 4:** The fourth relationship is between **organisational factors and cloud adoption**. This relationship ensures that IT investments produce business value as well as mitigate the risks and challenges associated with IT. At this stage, the cost of adoption, migration, acquisition, customisation, uncertainty and cost of data confidentiality and availability loss is determined and calculated. Taking into consideration the overall cost performance required for the adoption of cloud computing in the public sector, the study supports that cloud models are cost-effective but require a huge upfront investment. The top management sums up all cost factors and presents the budget to the finance department in the organisation. The finance department approves and enables the budget.

**Relationship 5:** The fifth relationship is between **adoption factors and security and privacy requirements and trust**. The stakeholders ensure that proper security controls that fulfil the security and privacy requirements are in place. The study reveals that cloud computing can only be trusted once proper security mechanisms are in place. This creates a positive working relationship between the cloud owner, cloud customers and cloud providers.

**Relationship 6:** The sixth relationship is between **technological enablers and cloud adoption**. Technology enablers promote cloud adoption. This ensures that cloud adoption is based on the needs and requirements of the government to address the goals and business sustainability.

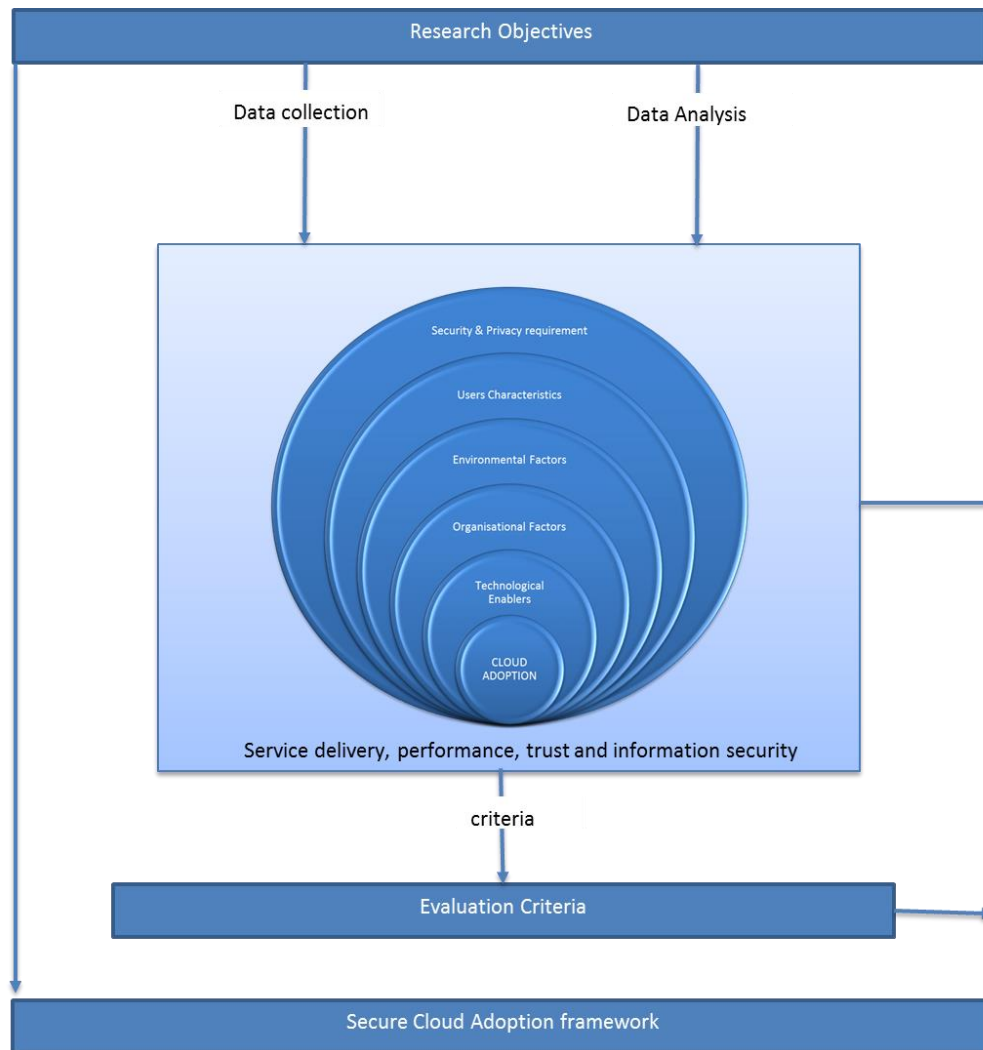
**Relationship 7:** The seventh relationship is between **cloud adoption and cloud implementation**. After the decision to adopt the cloud solution, the next phase is the implementation. Implementation plan and process should be addressed. Implementation is the crucial stage for users to access the cloud services deployed. This ensures that the cloud services to be accessed are available and that all security and privacy requirements are implemented. For the users to trust accessing the cloud services (technology) the following security controls should be in place: confidentiality, availability

and integrity of data or information, authentication, authorisation, access control, transparency and compliance.

**Relationship 8:** The eighth relationship is between **cloud implementation and management (service monitoring, evaluation, auditing, etc.)**. At this stage, it involves governance, which provides an integrated governance, management and process frame to implement and execute information security. This sums up and covers all the security issues and ensures compliance to all components needed to implement cloud computing. The framework is also reviewed and evaluated by the expert reviewers. It ensures continuous support, service monitoring, evaluation, auditing, security management and trust management.

#### **6.2.4.4 *Tentative design***

A tentative design is developed and implemented in this stage. Figure 6-8 shows the conceptual design of all the links among the different components and it also shows how cloud computing adoption is influenced by this component. This conceptual design can help expert reviewers to review the framework based on technological availability, awareness, knowledge and skills of the factors affecting cloud adoption.



**Figure 6-8: Conceptual Design**

The conceptual design is further demonstrated through the implementation guidelines, Table 6-2 presents guidelines and how these guidelines are applicable to this study.

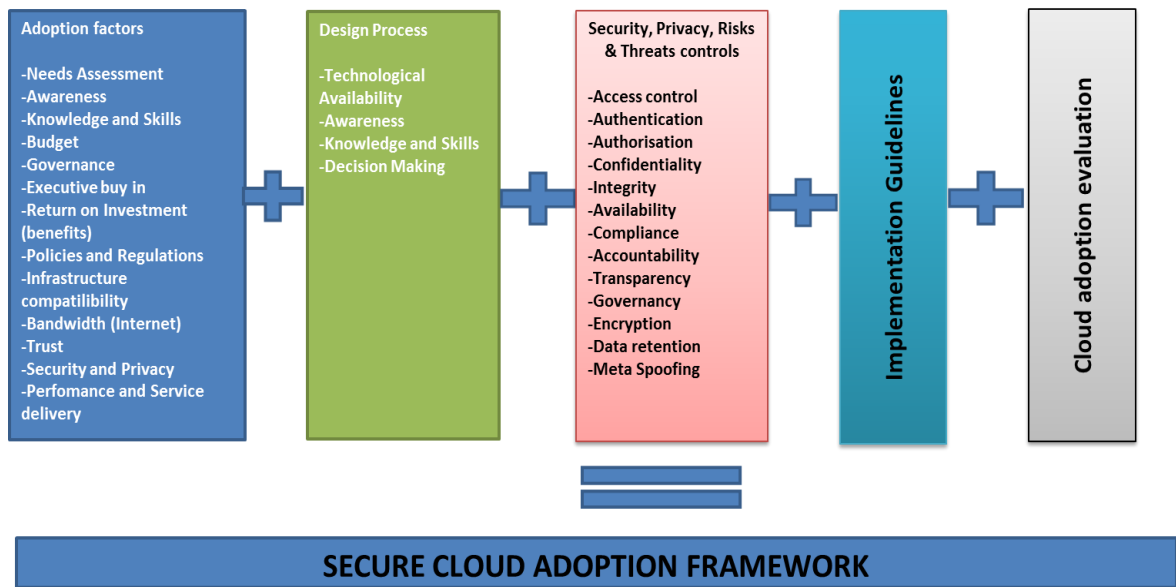
**Table 6-2: Guidelines of the Framework**

Implementation stages	guidelines	Implementation in this study
<b>Stage1: Identify factors affecting cloud adoption</b>		<p>The factors affecting cloud adoption were identified in Chapter 2 during literature review and confirmed by the study in chapters 5 &amp; 6. These components were grouped into four factors:</p> <ul style="list-style-type: none"> <li>✓ <b>Organizational factors:</b> needs assessment, executive management buy-in, return on investment (benefits),</li> </ul>

	<p>governance, budget, skills, trust, privacy and information security</p> <ul style="list-style-type: none"> <li>✓ <b>Technological enablers:</b> Infrastructure compatibility, bandwidth, security, performance, service delivery, trust and privacy.</li> <li>✓ <b>Environmental factors:</b> Policies, regulations, service providers and governance</li> <li>✓ <b>User characteristics:</b> Acceptance, awareness, expectations, knowledge and skills</li> </ul>
<b>Stage2:</b> <i>Establish cloud adoption baseline.</i>	<p>Data collected is analysed and used as recommendation for improvement:</p> <ul style="list-style-type: none"> <li>✓ Technology acceptance and awareness</li> <li>✓ Develop cloud security policies</li> <li>✓ Ensure compliances of policies and regulations</li> <li>✓ Technology compatibility and services availability</li> <li>✓ Security control measures in place</li> <li>✓ Budget allocation</li> </ul> <p>• This stage identifies what needs to be improved in adopting cloud.</p>
<b>Stage3:</b> <i>Implementation</i>	This stage uses the evaluation results. The technology intervention is implemented.
<b>Stage4:</b> <i>Evaluating</i>	The cloud technology is evaluated after implementing the changes.
<b>Stage5:</b> <i>Monitoring, auditing, security management, updating and continuous support</i>	After the evaluating plan is in place, the performance of the technology will be constantly monitored, audited and ensures security against threads and risks. The cloud technology should also be up to date with upgrades and new version releases. The study also reveals that continuous support from the vendors (cloud providers) is very important.

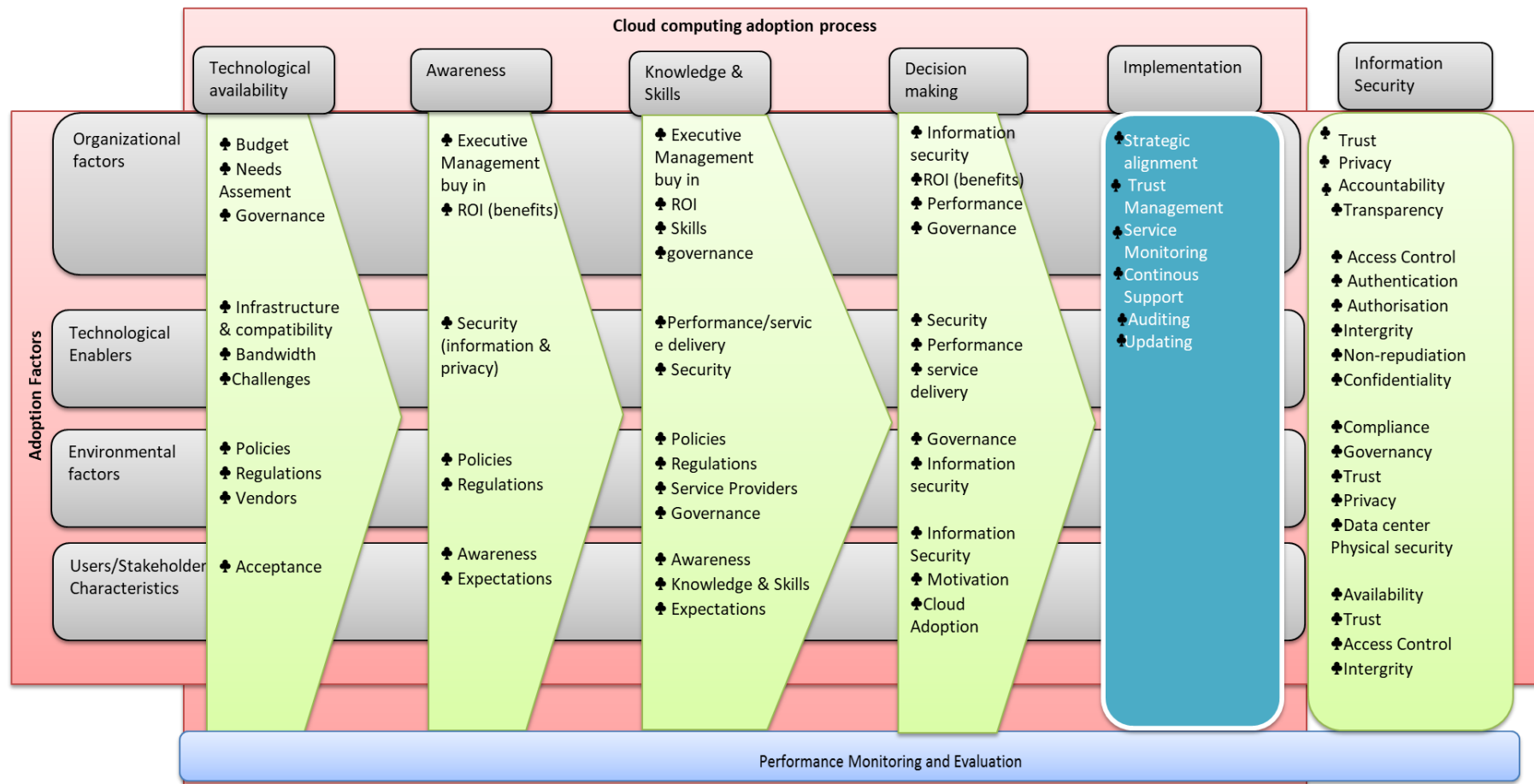
#### 6.2.4.5 Framework consolidation

Framework consolidation involves putting together all the identified components of the framework. Figure 6-9 presents the composition of all the components identified and the framework presented in Figure 6-10. This aims to answer the last question of the study: How can Namibia position herself with minimum risks on the cloud?



**Figure 6-9: Composition of All Components**

Figure 6-10 present the proposed framework for adopting cloud computing. This achieve the study objective “to propose a secure framework for cloud adoption in the Namibian government IT departments”. The framework is presented in Figure 6-10.



**Figure 6-10: A Secure Cloud Adoption Framework**



## 6.2.5 PHASE 4: Theoretical Demonstration

In this phase, the study demonstrates how to use the artefact to solve the problem. The researcher points out the benefits of cloud computing. The Namibian government IT departments, including RCs, can access central resources via cloud-based IT infrastructure. The framework provides guidelines on how to securely access these resources. IT experts no longer need to travel long distances to solve problems. Information is readily available everywhere. Proper policies are in place.

The case studies mentioned in Chapter 4 of this study are used as examples to demonstrate the implementation of the Secure Cloud Adoption Framework presented in Figure 6-14. Based on the suggested framework guidelines, the three used cases are mapped to the framework implementation guidelines provided in Table 6-2.

### Stage 1: Identify factors affecting cloud adoption

The first stage is to identify factors affecting cloud adoption in an organisation based on the proposed adoption process factors: Firstly, the organisational user/stakeholder characteristics involved in cloud computing adoption are defined. The cloud adoption team roles are defined in Table 6-3.

**Table 6-3: Cloud Computing Adoption Team Roles Defined**

Cloud Computing Adoption Team	Roles	Outputs
OPM	Legally own government cloud	Define policies, select relevant security dimensions and requirements
Directors and deputy directors	<ul style="list-style-type: none"><li>- Make decisions</li><li>- Assess cloud-based services</li><li>- Approve budget</li></ul>	<ul style="list-style-type: none"><li>- Influence decision making</li><li>- Identify services to implement on the cloud</li></ul>

Cloud Service Provider Cloud Experts	Provides IaaS and IaaS cloud services and advise accordingly	Deliver cloud computing services
Migration cloud experts Systems administrator System analyst IT technician	Execute the framework	- Implement - Integrate and migrate to cloud services
Experts review Government employees Internal IT auditors Security experts	Monitor, evaluate and audit the framework	- Ensure compliance of policies and security controls - Verification of service level agreements
OPM OMAs/MURD/RCs/DF	Implementation agencies	Implementations and deployment of the secure framework

In stage one, the most crucial component is to determine the needs and expectations of the Namibian government IT departments by defining the factors affecting cloud adoption as depicted in Table 6-4.

**Table 6-4: Factors affecting cloud adoption**

<b>Organisational Factors</b>	
<b>Needs assessment</b> (Performed by the deputy directors, chief system administrator/system analyst, security experts and cloud providers)	<ul style="list-style-type: none"> <li>-Identify services to migrate to the cloud e.g. IaaS and SaaS</li> <li>-Classification of information asset security categories: official, secret, top secret</li> <li>-Determine risk profiling</li> <li>-Does cloud computing innovation meet the departmental objectives</li> <li>- internal competency skills</li> <li>-The departments can sustain themselves</li> <li>-IT staff skilled to assist the users</li> </ul>
Executive management buy-in (OPM and MURD IT directors, deputy directors, chief system analyst/system administrator/analyst programmers)	<ul style="list-style-type: none"> <li>-Cloud computing is presented to IT directors, deputy directors and chief system analyst/system administrator/analyst programmers.</li> <li>-The executive management understand and grasp the value of the technology</li> </ul>

	<ul style="list-style-type: none"> <li>-Based on strategic planning and decisions making, the management supports the initiative.</li> <li>-Motivate for approval and implementation</li> <li>-Draft the Service Level Agreement terms and conditions</li> </ul>
Expectations (IT technicians and government employees)	<p>This is in line with organisation operations and may include:</p> <ul style="list-style-type: none"> <li>-Reduced IT infrastructure cost</li> <li>-Flexibility and scalability</li> <li>-Improved service delivery</li> <li>-Availability of cloud services to the RCs</li> <li>-Well defined security policies</li> <li>-Maximise resource utilisation</li> <li>-Cost effective</li> </ul>
Governance (OPM, cloud experts and audit committee)	<ul style="list-style-type: none"> <li>-Strategically align the cloud infrastructure to the Namibian national information technology's mission, needs and goals</li> <li>- assuring that the cloud adoption strategy delivers benefits and provides value</li> <li>-OPM ensures that resources are available and managed well</li> <li>-OPM monitors and measures the progress on the IT departmental performance towards cloud adoption</li> <li>-The procurement unit and audit committee ensures that there was is transparency in the decision making</li> <li>-Ensures that the service provider understand the government strategy</li> </ul>
Benefits	<p>Maximise service delivery, reduce cost, increase performance, eliminate lengthy procurement process, increase effectiveness, centralised resources, enhanced information availability, flexibility, disaster recovery, improved storage space, reduction in IT complexities, reduction in IT experts, systems integration, software legacy, auditing, environmental friendliness and the ability to launch rapidly which is a great return on investment to the Namibian government.</p>

Budget (IT directors and deputy directors)	<ul style="list-style-type: none"> <li>-Government cloud computing cost the project and avail budget for cloud computing implementation</li> <li>-The budget should include feasibility study cost, initial cloud computing acquisition budget and service level agreement cost</li> </ul>
Skills	<ul style="list-style-type: none"> <li>-Cloud Service Providers train the IT staff</li> <li>-Conduct training with all users</li> </ul>
Privacy and information security (IT directors, deputy directors and security officers)	<ul style="list-style-type: none"> <li>-Determine the privacy and security requirements</li> <li>-Select relevant security dimensions (availability, authenticity, confidentiality, privacy, trust management, accountability, transparency and identity management)</li> </ul>
<b>Technological Enablers</b>	
Infrastructure readiness (OPM and MURD IT directors, deputy directors, chief system analyst/system administrator/analyst programmers)	<ul style="list-style-type: none"> <li>-Reliable and electricity</li> <li>-Internet speed</li> <li>-List systems to be rolled over</li> <li>-Rollover plan</li> </ul>
Infrastructure compatibility (OPM and MURD IT directors, deputy directors, chief system analyst/system administrator/analyst programmers)	<ul style="list-style-type: none"> <li>-Assess the compatibility issues regard to the existing systems and applications</li> </ul>
Bandwidth	<ul style="list-style-type: none"> <li>-Upgrade bandwidth at regional councils and constituencies</li> </ul>
Security (security experts)	<ul style="list-style-type: none"> <li>-The Namibian government then establishes security requirements</li> <li>-Select relevant security dimensions e.g. availability, integrity, confidentiality, privacy</li> </ul>
Service delivery	<ul style="list-style-type: none"> <li>-CSP and implementation team ensures that the cloud system is performing as intent too.</li> <li>-Cloud services are reliable and always available</li> </ul>
<b>Environmental Factors</b>	
Policies Regulations	<ul style="list-style-type: none"> <li>-OPM in collaboration with other government OMAs, draft the recommended policies: cyber security policy, cloud governance policy, IT cloud legislation, cloud implementation guidelines, cloud</li> </ul>

	<p>computing policy, Technology integration policy and cloud security alliance</p> <p>-The implementation team ensures that all laws and regulations related to cloud computing adoption should be adhered to.</p>
Cloud Services Providers (CSP)	<p>-The role of the CSP is to advise accordingly.</p> <p>-OPM relies on the CSP's experience, skills and the ability to deliver the services.</p> <p>-Ensures that services are available to RCs, MURD and DF throughout.</p>
Governance	<p>-Compliance of IT cloud legislation and policies</p> <p>-Service monitoring and auditing</p>
Information Security	<p>-Ensures data security</p> <p>-Compliance with all standards</p> <p>-Trust and Privacy is maintained through trust management and national data protection laws</p>
<b>User Characteristics</b>	
Acceptance	-The users have accepted that cloud computing is useful and easy to use.
Awareness/knowledge	-Implement awareness campaigns to capacitate users
Expectations (IT technicians and government employees)	-Bringing service closer to the people
Skills	<p>- The right skills and knowledge experts are needed for the implementation of cloud adoption.</p> <p>-Train IT experts</p>

## Stage 2: Establish cloud adoption baseline

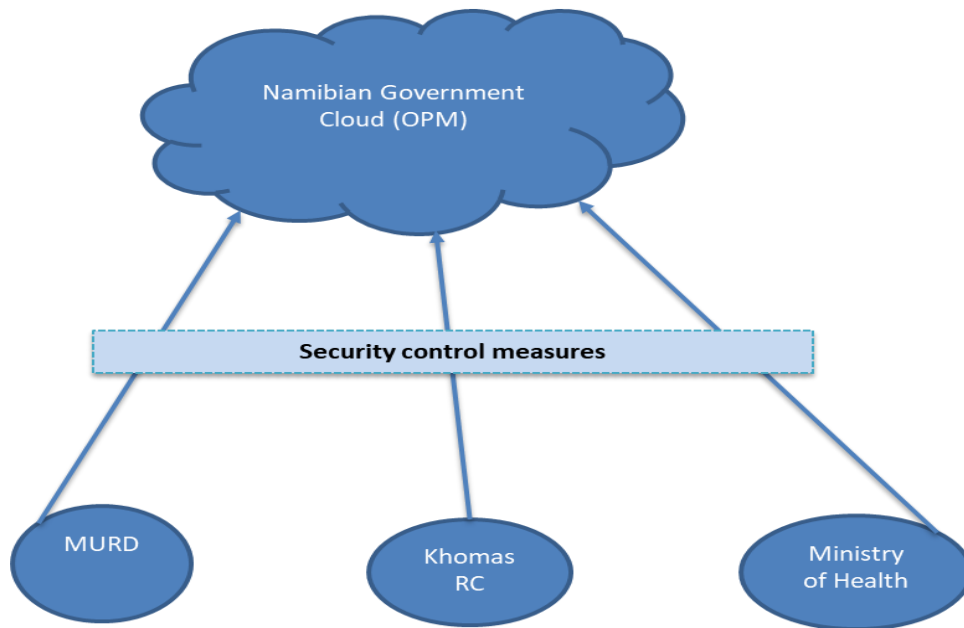
At this stage, the cloud adoption team (deputy directors, chief system administrator/system analyst, system administrator, system analyst, analyst programmer and cloud providers) establish a cloud baseline by ensuring that all activities required in stage 1 are analysed, completed and improve any gap identified:

- ✓ Strategic alignment to the government's mission and vision

- ✓ Technology accepted and all stakeholders are aware
- ✓ Classification of information assets based on data sensitivity and risks involve
- ✓ Cloud policies and regulations developed
- ✓ Compliances of policies and regulations
- ✓ Technology compatibility and services availability
- ✓ Security Control measures in are in place
- ✓ Budget allocated
- ✓ Experts capacitated

### Stage 3: Implementation

This stage utilises the evaluation results. The technology intervention is being implemented. The organisations are made aware and best practices are in place. An example of the cloud implementation is illustrated in Figure 6-11.



**Figure 6- 11: Namibian Cloud Implementation Illustration**

The roles of the cloud adoption team in the implementation are described as follows:

#### a. Office of the Prime Minister

OPM's mandate in ICT management is as explained in Chapter 4, to facilitate the process of formulation of policy and implementation of programmes within the government and the Public Service as a whole and to provide operational data service, develop and maintain systems and investigate OMAs' computers and systems' needs. Hence, OPM is the leading government agency that approves, oversees and coordinates the implementation of all developmental initiatives within the Namibian government IT departments.

OPMs' major role in adopting cloud-based services in the Namibian government is defining appropriate policies, selecting correct security dimensions and requirements currently, OPM is entrusted with IT infrastructure, and will also legally own the Namibian government cloud-based infrastructure.

#### **b. Directors and Deputy Directors**

In the Namibian government IT departments, the senior management team comprises directors, deputy directors and senior systems administrator/system analyst. This category manages the general services of all departments, plans, budgets and monitors all departmental IT activities and mostly approves all decision making in the entire department.

According to Kaisler et al. (2012), adopting cloud computing infrastructure is a major step and requires decisions in three categories service, system and application. Service refers to how the service is provided by assessing the user's view of the cloud computing. The system category implies how the application uses the cloud computing by assessing the infrastructural issues. The last category, application implies how the application is mapped in cloud computing environment by assessing how the application is mapped to the infrastructure.

These users are very crucial in the cloud-based adoption framework, as they are influential in decision making whether to adopt or not to adopt cloud computing. They will assess the cloud-based services and identify services to migrate to cloud computing systems. They are accountable for the implementation team.

#### **c. Cloud Service Provider**

The cloud service provider is the organisation that will provide cloud-based services and make the services available to the government employees. This provision of services is defined according to the requirements provided by the cloud owner (OPM), and normally described in the service level agreements (ENISA, 2015). This team comprises cloud experts.

**d. Experts review, researcher and government employees: internal auditors, security experts, etc**

This team ensures that the framework complies with all the defined appropriate policies, security controls and meets all the requirements. Their main role is to monitor, evaluate and audit the framework. Their assessment and review of the framework promotes, strengthens and ensures the urge to adopt cloud computing services. They are also responsible for verifying SLA between cloud service providers and cloud owners.

**e. Migration cloud experts, system analyst, system administrator and IT technician**

This team executes the framework. After decision-making, monitoring and evaluation of the framework, this team is then instructed by decision-makers, in collaboration with the migration cloud experts, to implement the secure framework. They ensure integration and migration of IT from traditional infrastructure to cloudbased infrastructure.

**f. OPM and OMAs/MURD/RCs/DF**

This team consists of the implementing agencies. Bringing service closer to the Namibian citizens. This involves creating awareness, implementing and deploying of the secure framework. They use the services provided by the cloud service providers.

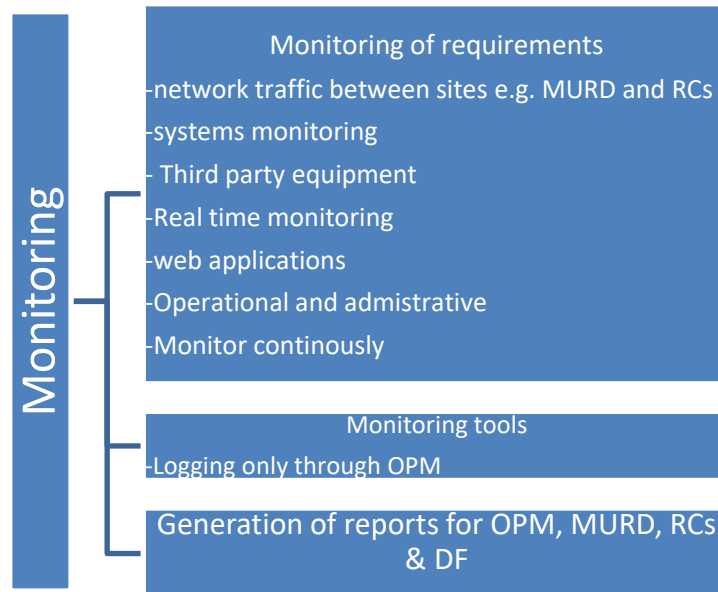
**Stage 4: Evaluating**

The cloud adoption framework is evaluated after implementing the changes.

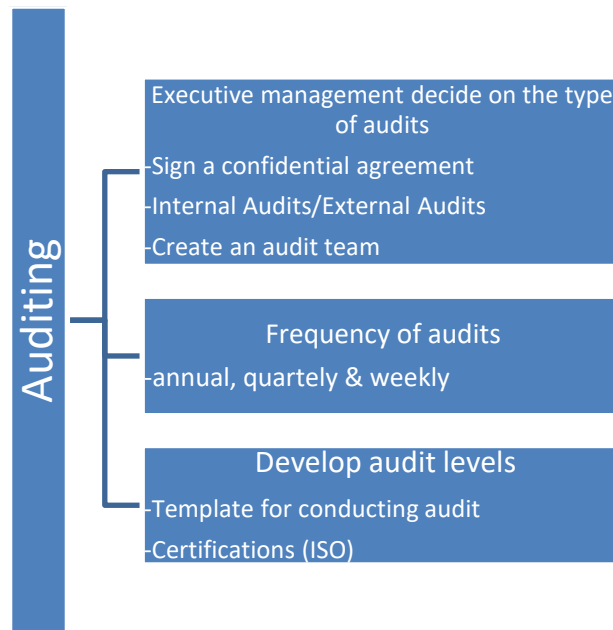


## Stage 5: Monitoring, auditing, security management, updating and continuous support

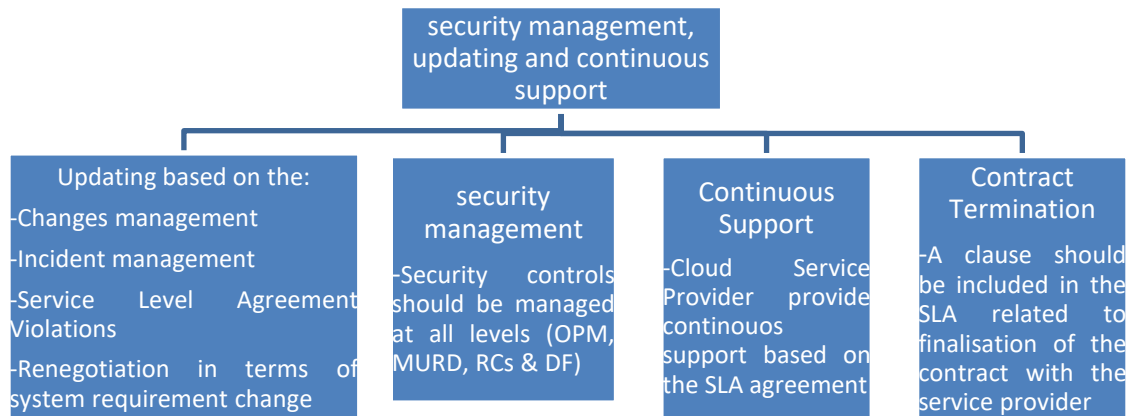
Figure 6-12 shows the events to be monitored, the monitoring tools and reports generated. Figure 6-13 shows the auditing process while Figure 6-14 elaborates on the security management, updating and continuous support.



**Figure 6-11: Cloud Services Monitoring Events**



**Figure 6-12: Cloud Services Auditing**



**Figure 6-13: Change Management**

### 6.2.6 PHASE 5: Framework evaluation

Evaluation of a framework is very important, as it seeks to produce judgment of value, measures the worthiness or determines the benefits (Pammett & Goodman, 2013). The

experts' review demonstrates measurements and observations that are accurate, reliable and valid. It gathers evidence systematically that the proposed framework is needed, it is fully developed, whether it meets the needs of those who will use it and makes suggestions that would improve the framework. The proposed secure cloud computing was evaluated using literature review and expert reviews.

#### **6.2.6.1 Expert Reviews**

An expert reviewer is an evaluator that uses his/her perceptual sensitivity, past experiences, refined insights and ability to assess an object and effectively communicate their assessments (Stufflebeam, 2000). An expert review is done to identify any issues pertaining to design in any product and to identify specific areas where these issues occur. In an expert review, the reviewer brings in his/her expertise in a given substantive domain, and also sometimes his/her personal choices or biases (Tory & Moller, 2005). Expert reviewers were drawn from professionals in the area of IT security, government IT departments, internal auditor, government policy development and cloud adoption framework research, as depicted in Table 6-5. All expert were unbiased as they had not participated in this study beforehand.

**Table 6-5: Participants' Profile**

<b>Participants' field</b>	<b>Position</b>	<b>Experience</b>
IT Security	IT Lecturers	Reviewer is a specialist in information security, user security, user experience, human computer interaction and ICT4D in underserved communities. The reviewer has a PhD in IT, MSc in Computer Science and BSc in Computer Science and Mathematics.

Government IT department	Directors and Deputy Directors (Head of departments)	Section 4.3.1  Note: Although these reviewers have the same position description and experiences as the data collection participants, these reviewers have not previously participated during data collection.
	Chief System Administrator/ System Analyst/ Analyst Programmer	
	System Administrator/ System Analyst/ Analyst Programmer	
	IT Technician	
Internal Auditing	Internal Auditors	
Government Policy development	Departmental Managers	Writes and develops reports and policy documents. The reviewer leads and manages policy officers within the policy and standards department and establishes and reviews standards. The reviewer conducts research, writes and develops a variety of reports and documents related to consultations, policy, guidance and standards. The reviewer provides information and guidance to management on all policy and standards issues.
Others	Security Officers	Specialise in cyber security.

#### **6.2.6.2 Framework evaluation tool**

Prior to conducting the reviews, the evaluation tool was developed and reviewed by the research supervisor and three other colleagues from different institutions. Piloting the evaluation tool was done to ensure that all questions were understood and to rectify any errors or design flaws.

The designed tool consisted of four sections. Firstly, the tool introduced the main aim of the tool and the demographic information of the participants. Secondly, the framework was evaluated on the needs assessment, benefits of cloud computing, budget, performance, technology acceptance, information security, policies and regulations, governance and compliance. Thirdly, the tool looked at cloud adoption, evaluating the relevance of technology readiness in the Namibian IT departments. Lastly, the tool evaluated the overall framework and any perceived suggestion. The research components were measured against a 4-point scale, from very important to least important, very relevant to least relevant or strongly agree to strongly disagree.

#### **6.2.6.3 Data Analysis**

Data analysis was categorised using predefined themes and data analysed under those themes. The analysed data were used as recommendations to improve and refine the SCAF framework. The evaluation tool was emailed to 25 experts and only 20 experts participated.

#### **6.2.6.4 Evaluation Findings**

##### **Demographic information**

The demographic information details collected on the background of the participants. Table 6-6 presents the participants' demographic information.

**Table 6-6: Expert Profiles**

<b>Position</b>	<b>Information security years of experiences</b>	<b>Years of experience in governance</b>
Academic: Prof/Dr/MSc	6-10	0 -5

Analyst Programmer, Chief System Administrator/System Analyst/Analyst programmer	0 – 5	0-5
Head of Information Technology	6-10	0- 5
Information Security Expert, Academic: Pro/Dr	11-20+	0- 5
Internal Auditors	11-20+	11- 20+
IT Technician	0- 5	0- 5
IT Technician	0- 5	0- 5
IT Technician	6- 10	0- 5
IT Technician	0- 5	0- 5
IT Technician	0-5	0- 5
System Administrator	0- 5	0- 5
System Administrator	0- 5	6-10
System Administrator	0- 5	0- 5
System Administrator	0- 5	0- 5
System Administrator	0- 5	0- 5
System Administrator	0- 5	0- 5
System Administrator	6- 10	0- 5
System Administrator	0- 5	6-10
System Administrator	6-10	6-10
System Administrator	6-10	6-10

## FRAMEWORK EVALUATION

This section assessed the proposed factors for SCAF. The findings reveal that most of the reviewers agreed that the proposed factors influencing the implementation of SCAF framework were very important. The factors are listed below and their score per factor.

### Needs assessment

The results revealed that most of the reviewers saw needs assessment as a very relevant factor to the organisation's needs in the adoption of cloud computing in the Namibian government, as shown in Table 6-7.

**Table 6-7: Relevance of Cloud Computing Benefits**

Needs assessment	Very Relevant	Relevant	Not Relevant	Least Relevant	Total
The department's IT infrastructure and requirements for the organisation's sustainability.	85%	15%	0%	0%	100%
The mapping of cloud computing adoption to the organisation's strategy, to ensure that the departmental objectives and expectations are achieved.	55%	40%	5%	0%	100%
Evaluate organisation's internal competency such as skills, management support, availability of infrastructure and resources for cloud adoption.	65%	30%	5%	0%	100%
The challenges of the existing service delivery framework	45%	40%	15%	0%	100%

### Benefits of cloud computing (return on investment)

In Table 6-8, the reviewers confirmed the study findings that the listed benefits were very relevant in influencing the adoption of cloud computing services in the Namibian government. However, 25% of the reviewers thought that reduced IT experts were not relevant.

**Table 6-8: Relevance of Cloud Computing Benefits**

Cloud computing benefits	Very Relevant	Relevant	Not Relevant	Least Relevant	Total

Flexibility	40%	50%	10%	0%	100%
Centralised resources	65%	25%	5%	5%	100%
Hardware utilisation	50%	30%	15%	5%	100%
Scalability of IT resources	60%	30%	10%	0%	100%
Greater IT efficiency and agility	75%	10%	15%	0%	100%
Cost reduction	55%	40%	5%	0%	100%
Increased performance and better functionality	55%	30%	15%	0%	100%
Rapid elasticity	50%	35%	15%	0%	100%
Protection, care and technical support	60%	35%	5%	0%	100%
Auditing and logging	55%	35%	10%	0%	100%
Reporting and intelligently	55%	40%	5%	0%	100%
Policies management	60%	25%	15%	0%	100%
Systems integration and software legacy	60%	30%	5%	5%	100%
Business continuity	55%	35%	10%	0%	100%
Regular backups and disaster recovery	55%	40%	5%	0%	100%
Maximise improved service delivery	20%	50%	15%	15%	100%
Accessibility of services	45%	40%	15%	0%	100%
Improved storage space	50%	40%	10%	0%	100%
Lengthy procurement process eliminated	30%	50%	20%	0%	100%
IT experts reduced	45%	25%	25%	5%	100%
Improved security	25%	65%	10%	0%	100%
Enhanced availability of information	65%	25%	5%	5%	100%
Environmental friendly	50%	30%	15%	5%	100%
Reduction in IT complexities	60%	30%	10%	0%	100%
Ability to launch rapidly	75%	10%	15%	0%	100%

Most of the reviewers strongly agreed and agreed that the benefits evaluated were applicable to the Namibian government service delivery. Table 6-9 presents the results and again the reviewers strongly disagreed that reduced IT experts was not important. This confirms findings of similar studies by Kundra (2011) and Wyld (2010).

**Table 6-9: Importance of Cloud Computing Benefits**

Cloud computing benefits	Strongly Agree	Agree	Disagree	Strongly Disagree	Total
Flexibility	25%	70%	5%	0%	100%
Centralised resources	40%	50%	5%	5%	100%



Maximise hardware utilisation	40%	50%	10%	0%	100%
Scalability of IT resources	25%	70%	5%	0%	100%
Greater IT efficiency and agility	55%	40%	5%	0%	100%
Cost reduction	50%	40%	10%	0%	100%
Increased performance and better functionality	45%	55%	0%	0%	100%
Auditing and logging	45%	55%	0%	0%	100%
Systems integration and software legacy	45%	45%	10%	0%	100%
Business continuity	50%	35%	15%	0%	100%
Regular backups and disaster recovery	70%	30%	0%	0%	100%
Improved service delivery	45%	45%	5%	5%	100%
Accessibility of services	55%	40%	0%	5%	100%
Improved storage space	40%	55%	5%	0%	100%
Lengthy procurement process eliminated	45%	35%	15%	5%	100%
IT experts reduced	35%	30%	25%	10%	100%
Improved Security	55%	40%	0%	0%	100%
Enhanced availability of information	55%	45%	0%	0%	100%
Environmental friendly	15%	65%	20%	0%	100%
Reduction in IT complexities	35%	45%	10%	10%	100%
Ability to launch rapidly	20%	70%	10%	0%	100%

## CHALLENGES

The findings (Table 6-10) show that most of the listed challenges of the framework are very relevant in influencing the adoption of cloud-based services in the Namibian government. However, the reviews rated political interferences, integration issues and initial cost as irrelevant or of least importance.

**Table 6-10: Relevance of Cloud Computing Challenges**

Challenges affecting the adoption of cloud	Very Relevant	Relevant	Not Relevant	Least Relevant	Total
Security issues	65%	30%	5%	0%	100%
Privacy issues	60%	40%	0%	0%	100%
Technology complexity	40%	40%	15%	5%	100%
Trust of where government data is stored	65%	25%	5%	5%	100%
Data integrity	50%	30%	15%	5%	100%
Political interferences	15%	40%	20%	25%	100%
Compliance issues	40%	35%	20%	5%	100%

Lack of performance/functionalities	35%	45%	20%	0%	100%
Lack of skills to assess and implement	40%	45%	10%	5%	100%
Integration issues	25%	50%	25%	0%	100%
Inadequate IT budget for volume licensing	55%	25%	20%	0%	100%
Legal implications	40%	40%	15%	5%	100%
Insufficient vendor service commitment/lack of expertise	55%	30%	15%	0%	100%
Limited bandwidth capacity	65%	25%	10%	0%	100%
Low service availability (downtime)	45%	40%	15%	0%	100%
Initial cost/budget	45%	30%	25%	0%	100%
Trust	40%	50%	5%	5%	100%
Policies to support cloud	55%	35%	5%	5%	100%
Cloud infrastructure security	60%	30%	5%	5%	100%

## Budget

Table 6-11 shows that SCAF will be cost-effective and will reduce cost in IT hardware infrastructure and maintenance costs, low budget allocation, travelling costs, and operational and software costs. Although some reviewers agree that SCAF will reduce cost, some disagree that it will not reduce telephone cost and upfront payment.

**Table 6-11: Cloud Adoption Cost Effectiveness**

Cloud computing cost effectiveness	Strongly Agree	Agree	Disagree	Strongly Disagree	Total
IT hardware infrastructure and maintenance cost	55%	40%	5%	0%	100%
Based on SCAF the Namibian government can have a low budget allocated to IT service delivery.	30%	55%	15%	0%	100%
Travelling costs	65%	20%	15%	0%	100%
Telephone costs	25%	35%	35%	5%	100%
Network upgrades cost	20%	35%	30%	15%	100%
Upfront payment	20%	30%	50%	0%	100%
Operational cost	15%	65%	20%	0%	100%
Software cost	50%	40%	10%	0%	100%

## Performance

The reviewers indicated that the performance indicators are very relevant in adopting cloud-based services in the Namibian IT departments as depicted in Table 6-12.

**Table 6-12: Performance Relevance**

<b>Technology Performance indicators</b>	<b>Very Relevant</b>	<b>Relevant</b>	<b>Not Relevant</b>	<b>Least Relevant</b>	<b>Total</b>
Scalability	40%	50%	5%	5%	100%
Reliability	65%	35%	0%	0%	100%
Service availability	70%	25%	5%	0%	100%
Bandwidth	80%	10%	10%	0%	100%

### **Technology acceptance**

Most reviewers strongly agreed that the perceived usefulness, such as improved performance, maximised service delivery in government, high flexibility in delivering services, enhanced effectiveness of IT experts on the job, met the Namibian government IT departmental needs such as solving backlog issues at the RCs and SCAF would be useful in supporting RCs and other remote areas will influence the cloud adoption as depicted in Table 6-13.

**Table 6-13: Perceived Usefulness**

<b>Perceived Usefulness</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Disagree</b>	<b>Strongly Disagree</b>	<b>Total</b>
Improve performance	45%	55%	0%	0%	100%
Maximise service delivery in government	50%	50%	0%	0%	100%
High flexibility in delivering services	45%	50%	5%	0%	100%
Enhanced effectiveness of IT experts on the job	55%	30%	10%	5%	100%
Meets the Namibian government IT departments needs such as solving backlog issues at the RCs	40%	50%	10%	0%	100%
SCAF will be useful in supporting RCs and other remote areas	60%	30%	10%	0%	100%

Most reviewers agreed that SCAF will provide easy guidelines for IaaS to be easily integrated with the traditional IT infrastructure, will be easy to use, will enable timeless services, stakeholders will have easy access to information and applications and that SCAF is easy to use as a tool for cloud service integration as shown in Table 6-14.

However, 5% strongly disagreed that the Namibian government IT departments would find cloud computing easy to use.

**Table 6-14: Perceived Ease of Use**

Perceived Ease of Use	Strongly Agree	Agree	Disagree	Strongly disagree	Total
Provides easy guidelines for Infrastructure as a Service to be easily integrated with the traditional IT infrastructure	35%	65%	0%	0%	100%
The Namibian government IT departments would find cloud computing easy to use	35%	50%	10%	5%	100%
SCAF will enable timeless services	30%	60%	10%	0%	100%
Stakeholders will have easy access to information and applications	35%	60%	5%	0%	100%
SCAF is easy to use as a tool for cloud service integration	25%	60%	15%	0%	100%

### Information security

As depicted in Table 6-15, majority of the reviewers evaluated the security controls as very relevant or relevant towards the adoption of cloud based services in the Namibian government.

**Table 6-15: Security Controls**

Information Security controls	Very Relevant	Relevant	Not Relevant	Least Relevant	Total
Identification and authentication management	75%	25%	0%	0%	100%
Authorisation and access control	75%	25%	0%	0%	100%
Confidentiality	80%	15%	5%	0%	100%
Integrity	65%	25%	10%	0%	100%
Non-repudiation	30%	55%	15%	0%	100%
Availability	65%	35%	0%	0%	100%
Compliance and audit	50%	50%	0%	0%	100%
Transparency	60%	25%	5%	10%	100%
Governance	40%	50%	10%	0%	100%
Accountability	55%	30%	15%	0%	100%
Trust management	50%	25%	15%	10%	100%
Network security	75%	25%	0%	0%	100%
Data centre physical security	80%	10%	10%	0%	100%
Monitoring and evaluation	65%	35%	0%	0%	100%

## Policies and regulations

Cyber security policy, cloud governance policy, cloud implementation guidelines, cloud computing policy and technology integration policy are considered as very important IT policies and regulations towards cloud adoption by most of the reviewers. Only 5% rated cloud governance policy, cloud implementation guidelines, cloud computing policy, cloud security alliance and government audit as not important as depicted Table 6-16.

**Table 6-16: Importance of Policies and Regulations**

<b>The implementation and operation of information security according to organizational policies and procedures.</b>	<b>Very Important</b>	<b>Important</b>	<b>Not Important</b>	<b>Least Important</b>	<b>Total</b>
Cyber security policy	80%	20%	0%	0%	100%
Cloud governance policy	80%	15%	5%	0%	100%
Cloud implementation guidelines	60%	35%	5%	0%	100%
Cloud computing policy	60%	35%	5%	0%	100%
Technology integration policy	45%	55%	0%	0%	100%
Cloud security alliance	70%	20%	5%	5%	100%
Government audit	55%	40%	5%	0%	100%

## Governance

As shown in Table 6-17, the reviewers evaluated governance as very important towards cloud adoption. Strategic alignment of IT infrastructure to the organization's mission, needs and goals and compliance of IT cloud legislation and policies were rated by the majority of reviewers.

**Table 6-17: Importance of Governance towards Cloud Adoption**

<b>Governance factors (set of responsibilities and practices by executing management in providing strategic</b>	<b>Very Important</b>	<b>Important</b>	<b>Not Important</b>	<b>Least Important</b>	<b>Total</b>

<b>direction, ensuring that objectives are met)</b>					
Strategic alignment of IT infrastructure to the organization's mission, needs and goals	65%	25%	0%	5%	100%
Value delivery: assuring that the cloud adoption strategy delivers benefits and provides value	55%	40%	0%	0%	100%
Resources Management: the availability and management of adequate resources	50%	45%	0%	0%	100%
Measurement of IT department performance to monitor progress towards cloud adoption	55%	30%	5%	5%	100%
Compliance of IT cloud legislation and policies	65%	30%	0%	0%	100%
Identifying controls to mitigate known risks	45%	50%	0%	0%	100%
Provision of support for efficiencies and continuous improvement	45%	45%	5%	0%	100%
Transparency in decision making	45%	45%	5%	0%	100%
Understanding and awareness of cloud computing risks, and effective and appropriate management of these risks.	55%	40%	0%	0%	100%
Stakeholders trust the government's strategy	35%	50%	10%	0%	100%
Service monitoring and auditing	45%	50%	0%	0%	100%

## Compliance

All the reviewers evaluated all the listed compliance factors in cloud adoption as very important or important. Compliance implies that all laws, policies, legislations, standards and requirements are adhered too. None of the reviewers considered any

of the compliance factors as not important or least important as evidence in Table 6-18.

**Table 6-18: Importance of Compliance Factors**

How important is this compliance factor in cloud adoption?	Very Important	Important	Not Important	Least Important	Total
Identifying local and international laws, regulations and external requirements to be adhered to	65%	35%	0%	0%	100%
Reviewing and adjusting IT policies, standards and procedures to ensure that legal, regulatory and contractual requirements are addressed and communicated	60%	40%	0%	0%	100%
Monitoring the compliance requirements of IT policies, standards, procedures and regulatory	70%	30%	0%	0%	100%
IT cloud legislation compliance	50%	50%	0%	0%	100%

### Cloud adoption

Before adopting the cloud technology, the organisation have to assess the technology readiness aspects in the organisation. Majority of the experts validated the framework that cloud adoption readiness assessment, development of national cloud adoption secure framework, Service Level Agreement, availability of IT infrastructure (compatibility and interoperability), strategic and operations planning, executive management buy in, broadband connectivity/bandwidth, electricity availability and reliability, compliance to regulatory requirements and policies, information security and implementation budget are very relevant or relevant factors of technology readiness that are relevant towards cloud adoption as depicted in Table 6-19.

**Table 6-19: Relevance of Technology Readiness**

How relevant are these factors in adoption of cloud computing?	Very Relevant	Relevant	Not Relevant	Least Relevant	Total
Cloud adoption readiness assessment	50%	45%	0%	5%	100%
Development of national cloud adoption secure framework	45%	55%	0%	0%	100%
Service Level Agreement	55%	40%	0%	5%	100%
Availability of IT infrastructure (compatibility and interoperability)	65%	30%	5%	0%	100%
Strategic and Operations planning	45%	55%	0%	0%	100%
Executive Management buy in	60%	40%	0%	0%	100%
Broadband connectivity/Bandwidth	85%	15%	0%	0%	100%
Electricity availability and reliability	55%	40%	0%	5%	100%
Compliance to regulatory requirements and policies	55%	45%	0%	0%	100%
Information Security	75%	25%	0%	0%	100%
Implementation budget	50%	45%	0%	5%	100%

**Overall framework evaluation**

This section of the evaluation presented factors to validate the overall performance of the framework. A total of 55% reviewers strongly agree that the framework is relevant and needed. While majority strongly agree or agree that the framework is efficient, operational, well designed, useful and valuable as shown in Table 6-20. Although 25% of the experts strongly agree and 40% agrees that the framework requires improvement, 35% of the reviewers disagree that the framework needs improvement.

**Table 6-20: Overall Framework Performance**

Overall the framework is	Strongly Agree	Agree	Disagree	Strongly Disagree	Total
Efficient	40%	55%	5%	0%	100%
Operational	20%	75%	5%	0%	100%
Well designed and developed	35%	55%	5%	5%	100%
Relevant and needed	55%	45%	0%	0%	100%
Useful	45%	55%	0%	0%	100%
Adaptable	35%	60%	5%	0%	100%
Requires improvement	25%	40%	35%	0%	100%
Valuable	25%	75%	0%	0%	100%



**Comments/Recommendations:**

- Expert 1:** Overall a well thought and detailed framework, however, have these few questions for clarification and adjustment observation later. By having an adoption factor of "Environmental factors," how do you envisage the separation of Internal and external environment be applied when your framework is adopted for use? (Internal environment can constitute management, people, process and technology for instance) Considering the "Information Security" attributes, from the way you have presented them there is a noticeable alignment to a specific "adoption factor" if that is the case, Why is Accountability not included under the list for "Users/Stakeholder characteristics" given the fact that it's aligned to "organisational factors" ? If what I have highlighted above is correct i.e. for alignment, just on the technical adjustment level, would recommend you revisit the adoption process "Knowledge & Skills" and properly align the adoption factors for "Technological enablers".
- Expert 2:** I believe office of the Prime Minister needs to implement/ set up a cloud of the government. Too many of our systems and information is in foreign hands.
- Expert 3:** Do we have a federal government in Namibia?

**6.2.6.5 Conclusion remarks**

The purpose of this section was to evaluate the proposed SCAF framework. The framework was evaluated by experts, their profiles are presented in Table 6-5 and analysed according to the predefined themes. The framework evaluation tool was formulated according to the study objectives and to determine if the proposed SCAF framework is needed, if it has been fully developed, and if it meets the needs of those who would use it. The online evaluation tool was designed using Google forms (Appendix G).

The findings reveal that most of the reviewers strongly agreed that the proposed factors influence the adoption and implementation of cloud computing in the Namibian IT departments are very important and relevant.

On the needs assessment, 5% of the reviewers suggested that evaluating the organisation's internal competency such as skills, management support, availability of infrastructure and resources for cloud adoption is not relevant, but the rest of the reviewers supports its relevance.

The relevance of assessing the existing service delivery challenges were considered not relevant by 15%, however 85% of the reviewers suggested that is very relevant or relevant and should remain part of the needs assessments.

Majority of the reviewers suggested that all proposed return on investments/benefits are very relevant and strongly agreed that they are important towards cloud adoption, however 30% of the reviewers feels that reduced IT experts is not relevant or is least relevant and not an important benefits towards cloud adoption. On the challenges, majority of the reviewers suggested that most of the challenges have to be mitigated as they affect the adoption of cloud. Although Political interferences, integration issues and initial budget is considered as not relevant challenges.

Although the results shows that adopting cloud is cost effective, 40% of the reviewers disagree that it will reduce telephone cost and 50% of the reviewers also disagree that it will reduce the upfront payment. This is in line with the study findings that cloud adoption requires a huge investment in upfront payments. Hence, upfront payment was removed as a cost effective sub-factor.

The findings also revealed that most of the reviewers agreed that scalability, reliability, service availability and bandwidth are very relevant. The framework is perceived as useful and ease of use as strongly agreed by majority of the reviewers. Most of the reviewers strongly agreed that the security controls such as identification and authentication management, authorization and access control, confidentiality, integrity, non-repudiation, availability, compliance and audit, transparency, governance, accountability, trust management, network Security, data centre physical security and monitoring and evaluation are very relevant.

All the proposed policies and regulations were considered as very important by most of the reviewers. The results also highlighted that governance towards cloud adoption is very important as rated by most of the reviewers. All reviewers recommend all the proposed compliance factors that is very important towards cloud adoption. The findings also considered technology readiness as very relevant as assessed by majority of the reviews.

The reviewers strongly agreed that the framework was efficient, operational, well designed and developed, relevant and needed, useful, adaptable and valuable. Furthermore, it met the needs of the Namibian government IT departments. In conclusion, the study found that the SCAF framework is essential and applicable to cloud adoption in the Namibian government IT departments.

#### **6.2.6.6 Refined Framework**

Based on the evaluation and validation processes, the suggestions and comments from the experts were carefully considered and addressed as areas of improvement. Some comments were already tackled earlier in the research, some influenced the changes in the framework and the rest were to do with the alignment of factors in the framework. This is presented in Table 6-21. The framework was refined accordingly. Overall, Expert 1 expressed that it was a well thought out and detailed framework.

**Table 6-21: Framework Evaluation Development Process**

<b>Evaluation Factor</b>	<b>Experts</b>	<b>Suggestions/Comments</b>	<b>Improvement made</b>
Environmental Factors	Expert 1	By having an adoption factor of "Environmental factors", how do you envisage the separation of internal and external environment would be applied when your framework is adopted for use?	The factors are clearly defined in the framework.
Information Security Controls	Expert 1	Considering the "information security" attributes, from the way you have presented them there is a noticeable alignment to a specific "adoption factor". If that is the case, why is accountability not included under the list for "users/stakeholder characteristics" given the fact	Accountability added as a security control under Users/Stakeholders characteristics.

		that it's aligned to "organisational factors"	
General	Expert 1	For alignment, just on the technical adjustment level, would recommend you revisit the adoption process "Knowledge & Skills" and properly align the adoption factors for "Technological enablers".	Proper alignments were made
Governance	Expert 2	I believe Office of the Prime Minister needs to implement/ set up a cloud of the government. Too many of our systems and information is in foreign hands.	Office of the Prime minister was purposely selected as a case study for this reason. Clearly explained in Chapter 4.
Policies and regulations	Expert 3	Do we have a federal government in Namibia?	No, we do not have federal government in Namibia. Federal government policy was removed from the list.
Overall Framework	Expert 1	Overall a well thought out and detailed framework	

Figure 6-15 presents the refined framework guidelines with the recommendations incorporated.

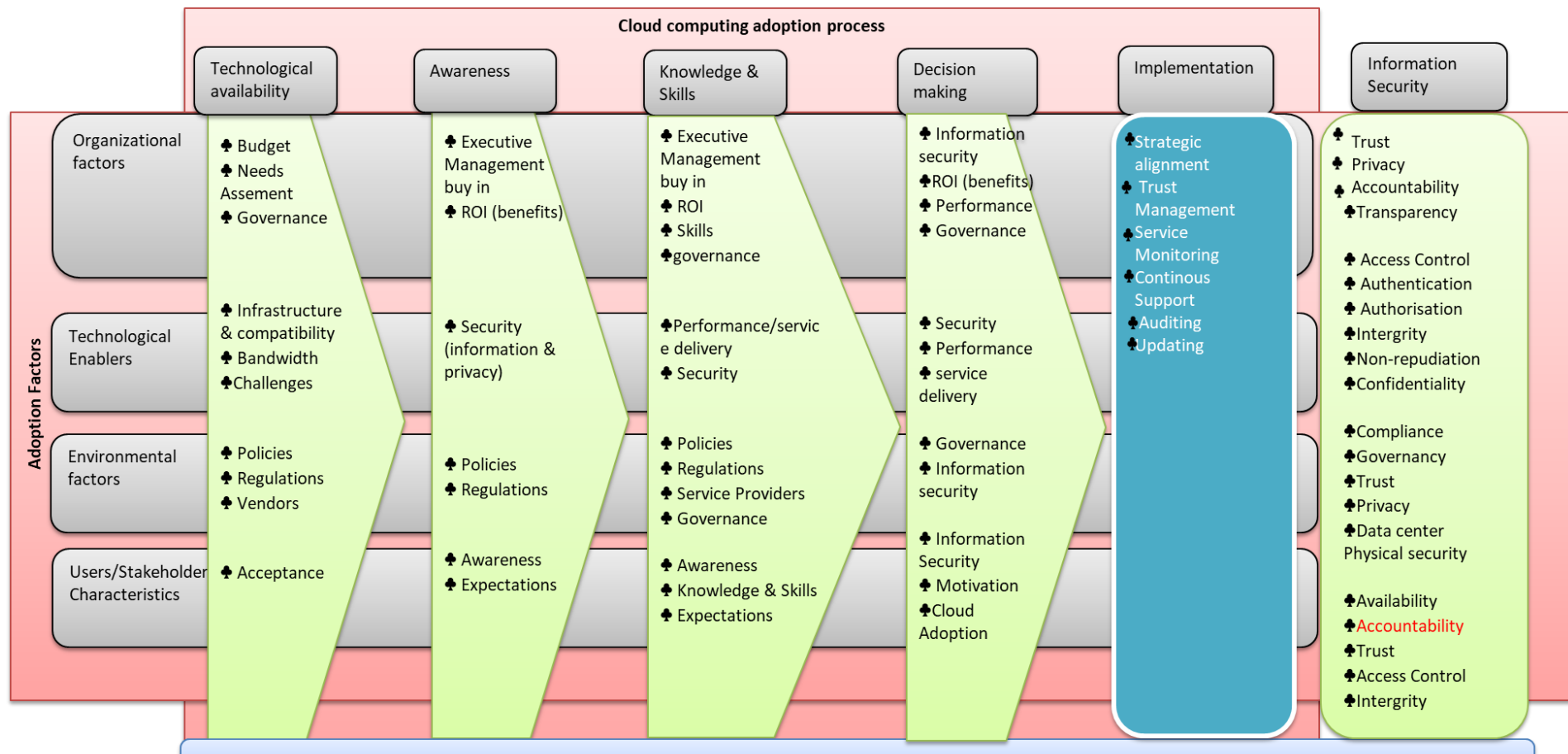


Figure 6-14: Refined Secure Cloud Adoption Framework

### **6.2.7 PHASE 6: Communication**

The contributions of this effort are presented in this thesis as well as disseminated in peer reviewed scholarly publication. The framework will be presented to the government institutions used as a case study.

### **6.3 Chapter summary**

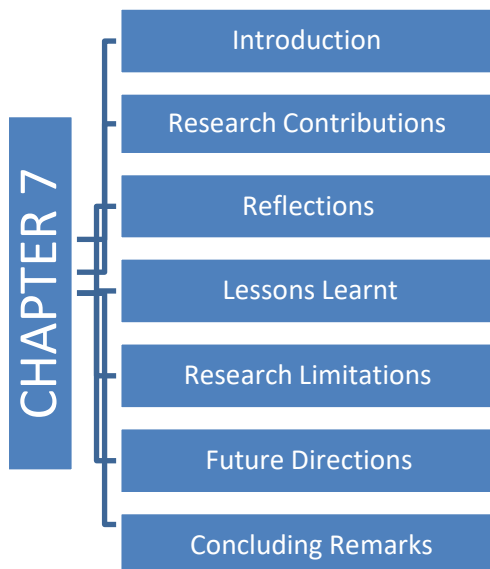
This chapter presented the process used to design the secure cloud adoption framework for cloud adoption in the Namibia government IT departments. It highlighted the factors affecting the adoption of cloud-based services and these factors include the technology enablers, organisational factors, and environmental factors and stakeholders' characteristics. Furthermore, the process and applicability of the framework development is also presented. The chapter also presented a positive validation on the evaluation of the proposed framework. The experts considered the proposed SCAF framework as important, relevant, useful, adaptable and valuable. Little improvement was made on the framework based on the experts' recommendations. Lastly, the quality of the framework and transferability through the documentation of tools was demonstrated.

The next chapter, Chapter 7 highlights the overall study conclusion and recommendations.

## CHAPTER 7: RECOMMENDATIONS AND CONCLUSION

### 7.1 Introduction

This chapter presents the research contributions, reflection, lessons learnt, research limitations, future directions and concluding remarks. The previous chapters discussed the problem, methodologies, literature studies, as well as the empirical study. The research problem was that the Namibian government ministries have IT departments that are characterised by a central headquarter department located in Windhoek, which supports several regions and constituencies. MURD, like other ministries, has physical servers and a variety of other network equipment deployed at the 14 RCs to provide Internet, email, webmail and mail to mobile services to the governors' offices and RCs. The servers also provide virtualised Windows Server services such as Application Server services, Domain Controller services, Software Update services, Antivirus services and Terminal services. To protect ICT equipment against hardware failures, MURD IT division employees travel long distances to do server maintenance, cabinet clean up, network connectivity setup between RCs and OMAs, and to solve problems at hand. Due to time, budget and staff constraints, users sometimes wait for long periods before ICT problems are solved. This chapter presents the researcher's view of the whole thesis, following the outline.



## 7.2 Research contributions

The study will contribute significantly to the Namibian government IT departments and the research community at large in the following ways:

- The SCAF framework will promote central resource management within the Namibia IT departments, this will reduce the costs of IT hardware infrastructure, travelling and operations.
- The SCAF framework can be used as a guide for migrating government traditional wired infrastructural to cloud infrastructural service.
- The secure cloud adoption framework will assist directors and deputy directors of Namibia government IT departments with decision making and directives on whether to consider adopting cloud for the effective use of technology.
- The framework evaluation of adopting cloud services in Namibia will assist in providing future guidelines on how to improve service delivery in Namibia government IT departments.
  - The SCAF framework increases productivity and efficiency in the Namibia IT departments' government and as well as the community at large.
  - SCAF will promote service deliveries in the entire Namibia government including all fourteen regions as stipulated in Chapter 2 and 6.
  - SCAF will provide guidelines on how can Namibian government IT departments securely position themselves on the cloud computing environment.
  - The proposed secure cloud adoption framework promotes the utilizations of new technologies in the Namibian IT departments, this can be applied to similar setups.
  - SCAF encourages the formulation, implementation and enforcement of policies such as cloud computing security and cyber security policies in the Namibia government.



### **7.3 Reflection**

This section presents the three types of reflections namely: scientific, methodological and substantive. According to Vaishnavi and Kuechler (2004), reflection is a DSR cognitive process that is carried out before the conclusion of the research. Scientific reflection focuses on generalisations of the contributions made. Methodological reflection describes the research process taken to come up with the framework while substantive reflection defines the study scope.

#### **7.3.1 Scientific reflection**

With new technology advancements evolving around the world every day, government institutions are forced to look for initiatives that can improve service delivery and ensure that the citizens get information timely. Cloud technology has tremendous benefits that can maximise service delivery in Namibian government IT departments, including all 14 regions countrywide. Despite the gains, technology is faced with security concerns, risks and challenges. The study reveals that these challenges can be mitigated through the implementation of proper security measures, policies and through trust management tools. This study proposed a framework that could guide the Namibian government on how to securely adopt cloud computing. The study identified and took into consideration four adoption factors namely; organisational factors, technological enablers, environmental factors and users' characteristics. The framework is positioned to assist with decision making, contribute to IT capacity building, act as a guideline and encourage the formulation, implementation and enforcement of policies such as cloud computing security and cyber security policies in the Namibian government.

#### **7.3.2 Methodological reflection**

When conducting research, a researcher is required to be neutral and unbiased. The study used a qualitative multiple case study research paradigm that typically allows for generalisation to other sites. The study could not use quantitative research methods, as they focus more on generating numerical data or statistics. The study used the DSR paradigm to design the framework. The DSR process outlines the problem statement of

the study as well as the presentation of other phases that lead to the development of the framework. Data were collected through questionnaire, literature review, interviews and expert reviews. Data content was analytically analysed and interpreted into meaningful results. The methods used for the study were best suited for the objectives of this study.

### **7.3.3 Substantive reflection**

The scope of the study focused on analysing and understanding the benefits of cloud computing as well as understanding how to mitigate the security risks and concerns accompanying the paradigm. This enabled the identification of the secure cloud adoption framework adoption factors (organisational factors, technological enablers and users' characteristics). These constructs of the SCAF enabled and informed the design of the evaluation tool for the experts. With the emerging technologies, government organisations are forced to follow suit by adopting technologies that are crucial to the organisation's core functions. The proposed SCAF is essential for the Namibian government IT departments, as it maximises service delivery and promotes centralises resources management.

#### **7.4 Lessons learnt**

Firstly, I have learnt about perseverance. Through this period of study and research, I have learnt the value of hard work and the need to persevere and stay the course to the end. During the long nights of writing, reading and going through research findings, sitting up at 2am one felt like giving up, calling off the whole thing, but I decided to stay on the course and complete the study for I convinced myself to do so.

Secondly, growth. I have grown tremendously during this period not only in knowledge but also in work ethics and determination. I have also learned that the ability to read and write English is not a measure of intelligence because there were many people I interviewed and spoke to on the issue of cloud computing in government who had a wealth of information and insights to share that they could only articulate elegantly in their own dialect.

Thirdly, I have learnt that criticism is good. The best thing that helped me improve and understand my work better during my dissertation writing process was constructive feedback from my supervisor. My supervisor was really committed to go through my work and provided me with feedback timely. She motivated me to overcome my limits and reach higher standards of this research.

Lastly, it is evidently clear that cloud computing is here to stay and is the future. Almost everyone has been touched or is already using services on the cloud. The reality is that many government institutions are already using cloud services without knowing it and without proper adoption frameworks in place. Be it Dropbox to exchange files with other government agencies or partial or online services in the cloud. Cloud computing services might be leaving government open to many security threats but also new opportunities. Through in-depth research, I have learned that those threats can be mitigated and the opportunities far outweigh the risks.

## **7.5 Research limitations**

This study encountered some limitations. To gain an in-depth understanding of the phenomena in context, the study sample size was confined only to IT experts from OPM, MURD, RCs and decentralised functions, as this was representative of all the other government ministries and departments, however, it can be transferable. This might not be fully representative of the different organs, as each has a unique function that usually complements the other functions. The findings of the investigated phenomenon in the Namibian context is not necessarily enough to generalise the opinions of all IT experts in Namibian government IT departments to all sectors. Secondly, the research was conducted on the IT experts who are knowledgeable in the IT fields and have deeper understanding of technologies. Policy decisions and framework reviews are made by specialists who hardly have a skill in IT, their opinions might differ from those of the findings, however through articulation on the applicability of the framework to the different roles in the governance of ICTs in government this may be overcome. The users might find it difficult to understand and interpret the findings. Thirdly, the proposed secure cloud adoption was only reviewed by different experts in the field, but not tested in practice. Future considerations are discussed next.

## **7.6 Future considerations**

In future, study could integrate all Namibian government IT departments to generalise the framework to the entire government. The framework will be implemented in the case site and evaluated over time as a pilot site before rolling it out to all Namibian government organs.

It is recommended that the proposed SCAF framework be revised continually to support any future technological advancements, applicability and implementations for any future development. In future, it would also be worthwhile to explore the readiness of the Namibian citizens of the studied IT departments to adopt and use cloud computing services.

Section 7.7 presents the concluding remarks.

## **7.7 Concluding remarks**

The overall aim of this study was to assess and investigate the benefits and challenges associated with adopting a cloud-based infrastructure service, especially focusing on security and propose a framework for secure cloud adoption in the Namibian government IT departments. The findings reveal that cloud computing offers benefits such as cost reduction, flexibility, centralised resources, IT efficiency, improved service delivery, hardware utilisation, data recovery, secure backups, advanced IT infrastructure, increased performance, availability of information and scalability. Namibian government IT departments can equally benefit from the mentioned benefits. However, this presents security issues and challenges, the greatest being privacy, secure transmission and lack of trust where data is stored. To securely adopt cloud computing services, the Namibian government needs to make well informed decisions based on the cloud technology, draft, cloud policies and regulations, deploy a cloud adoption team, implement security controls, upgrade network bandwidth around the 14 regions, ensure stable reliable electricity availability, perform needs assessment and conduct a feasibility study prior to implementation. The study emphasises that all mentioned factors of the framework should be addressed for the successful implementation of SCAF. The framework will be distributed to the OPM and MURD.

Table 7-1 summarises and presents how the research objectives were addressed and the outcomes.

**Table 7-1: Research Question, Answers and Evidence**

Research question	Answer	Evidence
1. What benefits does cloud computing yield to Namibia's government future IT infrastructure?	1. Cost reduction, flexibility, centralised resources, IT efficiency, improved service delivery, hardware utilisation, data recovery, secure backups, advanced IT infrastructure, increased performance, availability of information and scalability.	Chapter 2, 5 and 6
2. What are the security issues and challenges in adopting cloud-based Infrastructure as a Service in Namibian government institutions?	2. Security issues, privacy issues, technology complexity, limited bandwidth capacity, initial cost and policies to support cloud.	Chapter 2, 5 and 6
3. To what extent are Namibian government IT departments ready to adopt cloud computing?	3. Majority of the Namibian government IT officials are familiar with cloud computing. The respondents show great positivity towards the cloud adoption readiness in Namibian government IT departments. Namibia government IT departments are ready to adopt cloud computing, however legal	Chapter 2, 4 and 5

	frameworks such as cloud security policy and cloud adoption strategy should be developed before implementing cloud adoption.	
4. In what ways can the Namibian government position itself to adopt cloud-based computing services with minimum security risks?	3. Motion	Chapter 2, 4, 6 and 7

The research objectives were successfully addressed and they have contributed solutions to the research community and guidelines to adopt cloud computing to the Namibian ICT governance. SCAF is transferable to other Namibian government OMAs' IT departments.

## REFERENCES

- Alshamaila, Y., Papagiannidis, S. & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management*, 26(3). <https://doi.org/10.1108/17410391311325225>
- Alshomrani, S. & Qamar, S. (2013). Cloud based e-government: benefits and challenges. *International Journal of Multidisciplinary Sciences and Engineering*, 4(6), 15–19.
- Amazon (2009). What's new 2009. Retrieved from: <https://aws.amazon.com/about-aws/whats-new/2009/>. Date accessed: 25 September 2009
- Archer, L.B. (1984). Systematic method for designers, in: Developments in design methodology, N. Cross (ed.), John Wiley, London.
- Arrington, M. (2009). "White House using Google Moderator for town hall meeting. And AppEngine. And YouTube," Tech Crunch. Retrieved from: <http://www.techcrunch.com/2009/03/24/white-house-using-google-moderator-for-town-hall-meeting/>. Date accessed: March 26, 2015.
- Awad, M. & Leiss, E.L. (2010). Paper Records and Electronic Audits. *Journal of eDemocracy & Open Government (JeDEM)*, 2(1), pp.69–78.
- Barratt, M., Choi, T.Y. & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of Operations Management*, 29(4), 329-342. DOI: 10.1016/j.jom.2010.06.002.
- Bhunu Shava, F. (2015). *A Framework to Evaluate User Experience of End user Application Security Features*. Nelson Mandela Metropolitan University.
- Borko, F. & Armando, E. (2010). *Handbook of Cloud Computing*. New York: Springer.
- Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. IDG Communications, Inc.
- Bryman, A. (2012). *Social Research Methods (4ed.)*. New York, United States: Oxford University Press.
- Bryman, A. (2013). Mixed-methods research: how to combine quantitative and qualitative research.
- Carr, P.J. (2003). The new parochialism: The implications of the Beltway case for arguments concerning informal social control. *American Journal of Sociology*, 108, 1249–1291.
- Charmaz, K. & Belgrave, L. (2002). Qualitative interviewing and grounded theory analysis. *The SAGE handbook of interview research: The complexity of the craft*, 2, p.2002.



- Creswell, J. & Clark, V.P. (2007). Choosing a mixed-methods design. *Designing and conducting mixed methods research*, pp.53–106.
- Creswell, J.W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). London: Sage Publications.
- Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13 (3), 319-340.
- Dawoud, W., Takouna, I, Meinel, C. & Plattner, H. (2009). Infrastructure as a Service Security: Challenges and Solutions, 4IDC Enterprise Panel, *Institute Potsdam*, Germany.
- Dooley, L. M. (2002). Case study research and theory building. *Advances in Developing Human Resources*, 4(3), 335-354.
- Eekels, J., & Roozenburg, N.F.M. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences, *Design Studies*, pp 197-203.
- ENISA. (2015). *Security Framework for Governmental Clouds*. <https://doi.org/10.2824/57349>.
- Eric, A.M. & Bob, L. (2010). *Executive's Guide to Cloud Computing*. Hoboken, New Jersey: John Wiley and Sons. PP. 40-102.
- Ertaul, L., Singhal, S. & Saldamli, G. (2010). Security Challenges in Cloud Computing. *Security and Management*, 36–42. <https://doi.org/10.1109/CloudCom.2014.171>
- Gangwar, H., Date, H. & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, 28(1). <https://doi.org/10.1108/JEIM-08-2013-0065>
- Garfinkel, S., & Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices. *IEEE Security and Privacy*, 1(1) 17-27 .
- Gasser, U., & O'brien, D. R. (2017). Governments and Cloud Computing: Roles, Approaches, and Policy Considerations. Retrieved from: <http://cyber.law.harvard.edu/research/cloudcomputing>. Date accessed: January 15, 2018.
- Glaser, B., & Strauss, A. (1967). The discovery of grounded theory: Strategies for qualitative
- Glick, B. (2009). Digital Britain commits government to cloud computing, *Computing*. Retrieved from: <http://www.computing.co.uk/computing/news/2244229/digital-britain-commits>. Date accessed: July 28, 2015.

- Golafshani, N. (2003). The Qualitative Report Understanding Reliability and Validity in Qualitative Research Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, 8(4), 597–606. Retrieved from <http://nsuworks.nova.edu/tqr>. Date accessed: October 8, 2015.
- Gopala, K. B., Vishnu, V. V. & Madhusudhana, R. (2009). "Service Oriented Architecture for E-Governance", Retrieved from [www.bptrends.com](http://www.bptrends.com). Date accessed: October 5, 2016.
- Grispos, G., Glisson, W.B. & Storer, T. (2013) Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization. *In: 21st European Conference on Information Systems*, 5-8 Jun 2013, Utrecht, The Netherlands.
- Hamlen, K., Kantarcioglu, M., Khan, L. & Thuraisingham, B. (2010). Security Issues for Cloud Computing. *International Journal of Information Security and Privacy*, 4(2), 39-51
- Hancock, B. (2002). An introduction to qualitative Research, Trent focus group. University of Nottingham
- Harfoushi, O., Akhorshaideh, A. H., Aqqad, N., Janini, M. A. & Obiedat, R. (2016). Factors Affecting the Intention of Adopting Cloud Computing in Jordanian Hospitals, 8(8), 88–101. <https://doi.org/10.4236/cn.2016.82010>
- Hart, K. (2009). "Tech firms seek to get agencies on board with cloud computing," *The Washington Post*. Retrieved from: [http://www.washingtonpost.com/wp-dyn/content/article/2009/03/30/AR2009033002848\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2009/03/30/AR2009033002848_pf.html). Date accessed: April 21, 2015.
- Hashemi, S., Monfaredi, K., & Masdari, M. (2013). Using Cloud Computing for E-Government: Challenges and Benefits. *International Journal of Computer, Information Science and Engineering*, 7(9), 579–586.
- Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19(2), 87–92.
- Hevner, A. R., Ram, S., March, S. T. & Park, J. (2004). Design Science in Information Systems research. *MIS Quarterly*, 28(1), 75-105.
- Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems, 22, 9–23. <https://doi.org/10.1007/978-1-4419-5653-8>
- Hicks, R. (2009). "The future of government in the cloud," *FutureGov*, 6(3), pp. 58-62.
- Hirschheim, R. & Klein, H.K. (2003). Four Paradigms of Information Systems Development. *Communications of the ACM*, 32(10), pp.1199–1216.

- Hoover, J.N. (2009). "Japan hopes IT investment, private cloud will spur economic recovery: The Kasumigaseki Cloud is part of a larger government project that's expected to create 300,000 to 400,000 new jobs within three years," InformationWeek, Retrieved from: <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=217500403>. Date accessed: May 15, 2016.
- Hox, J.J. & Boeije, H.R. (2005). Encyclopedia of social measurement, pp. 593 – 599
- Hsieh, H. F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. Qualitative Health Research, 15, 1277-1288. <http://dx.doi.org/10.1177/1049732305276687>
- Hughes, D. (2007). Participant observation in health research. Researching health: Qualitative, quantitative and mixed methods.
- IBM (2009). Blue Cloud Initiative Advances Enterprise Cloud Computing. Retrieved from: <http://www-03.ibm.com/press/us/en/pressrelease/26642.wss>. Date accessed: March 26, 2017.
- IDC (2008), Cloud Computing is the Big Change in IT Retrieved from: [http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-industry-trends-FISMA\\_ISPAB-Dec2008\\_B-Whyman.pdf](http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-industry-trends-FISMA_ISPAB-Dec2008_B-Whyman.pdf). Date accessed: April 6, 2015.
- ISACA (2010) COBIT Framework for IT Governance and Control; ISACA, Retrieved from: <http://www.isaca.org/Knowledge-Center/COBIT/pages/Overview.aspx>. Date accessed: 25 September 2017
- ISACA. (2011). Introduction to the business model for information security. Rolling Meadows, IL:ISACA. Retrieved from: [http://www.isaca.org/knowledge-center/research/documents/introduction-to-the-business-model-for-information-security\\_res\\_eng\\_0109.pdf](http://www.isaca.org/knowledge-center/research/documents/introduction-to-the-business-model-for-information-security_res_eng_0109.pdf). Date accessed: February 13, 2017.
- Islam, M. M., Morshed, S. & Goswami, P. (2013). Cloud Computing : A Survey on its limitations and Potential Solutions, *IJCSI International Journal of Computer Science Issues* 10(4), 159-163.
- ITGI (2007). COBIT 4.1: Framework, Control Objectives, Management Guidelines and Maturity Model. IT Governance Institute (ITGI)
- Kaisler, S., Money, W. H., & Cohen, S. J. (2012). A Decision Framework for Cloud Computing. <https://doi.org/10.1109/HICSS.2012.52>
- KPMG Advisory N.V. (2011). From Hype to Future: KPMG's 2010 Cloud Computing Survey, 44. Retrieved from <http://www.kpmg.com/ES/es/ActualidadNovedades/ArticulosyPublicaciones/Documents/2010-Cloud-Computing-Survey.pdf>. Date accessed: November 15, 2016.

- KPMG. (2012). Exploring the Cloud - A Global Study of Governments' Adoption of Cloud, 46.
- Krauss, S.E. & Putra, U. (2005). Research Paradigms and Meaning Making: A Primer. *The Qualitative Report*, 10(4), pp.758–770.
- Kuldeep, V., Shravan, S. & Amit, R. (2012). "A Review of Cloud Computing and E-Governance", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol2, Issue 2.
- Kumar, K., Liu, J., Lu, Y. H. & Bhargava, B. (2013). A survey of computation offloading for mobile systems. *Mobile Networks and Applications*, 18(1). <https://doi.org/10.1007/s11036-012-0368-0>
- Kundra, V. (2010). State of public sector cloud computing. Washington, DC: Chief Information Officer (CIO) Council. <http://doi.org/10.1177/089976409102000202>
- Kundra, V. (2011). Federal cloud computing strategy, the White House, Washington DC.
- Kuyoro, S. O., Ibikunle, F. & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks*, 3
- Li, et al. (2015). Widespread Rearrangement of 3D Chromatin Organization Underlies Polycomb-Mediated Stress-Induced Silencing. *Mol. Cell* 58(2): 216-231.
- Li, X. (2010). Security Analysis on an Elementary E-Voting System, *IJCSNS* 10(10), pp.128–132.
- Low, C., Chen, Y. & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems*, 111(7), 1006–1023. <https://doi.org/10.1108/02635571111161262>
- Mahafuz, A. A. & Sakibur, R. (2011). "Implementing E- Governance in Bangladesh Using Cloud Computing Technology", BRAC University, Dhaka, Bangladesh.
- Mahlindayu Tarmidia, S. Z. A. R., Bakhtiar, A. & Rusli, A. R. (2014). Cloud computing awareness and adoption among accounting practitioners in Malaysia. *Mahlindayu Tarmidi et Al. / Procedia - Social and Behavioral Sciences* , 164, 569 – 574. Retrieved from [https://ac.els-cdn.com/S1877042814059679/1-s2.0-S1877042814059679-main.pdf?\\_tid=5ef2b578-b6ac-4bee-9c33-b6b23f16046f&acdnat=1521699968\\_89455d666e7a9f84c41502abeddd6647a](https://ac.els-cdn.com/S1877042814059679/1-s2.0-S1877042814059679-main.pdf?_tid=5ef2b578-b6ac-4bee-9c33-b6b23f16046f&acdnat=1521699968_89455d666e7a9f84c41502abeddd6647a). Date accessed: March 4, 2017.
- Maxwell, J.A. (2012). Qualitative research design: An interactive approach: An interactive approach, Sage.
- Mell, P. & Grance, T. (2009). 'The NIST Definition of Cloud Computing', *Communications of the ACM*, 53(6), 50.

- Mitchell, J. C. (2000). *Case and situation analysis*. In Gomm, R., Hammerlsey, M. & Foster, P. (Eds), *Case study method: Key issues, key texts* (pp. 165-186). Thousand Oaks, CA: Sage
- Mitchell, K., D'Arcy, J., Crowell, C. & Van Bruggen, D. (2014). An exploratory investigation of message person congruence in information security awareness campaigns. *Computers and Security*, 43: 64 - 76.
- Mitrovic, Z. & Klaas, V. (2012). The perceived benefits of introducing M-government services in the Western Cape. *Zawww 2012*.
- Mitrovic, Z. & Klass, N. (2013). The perceived benefits of introducing Cloud Computing based M- government services in the Western Cape. In 15th Annual Conference on World Wide Web Applications (ZA-WWW2013), Cape Peninsula University of Technology September.
- Mohammed, F., & Ibrahim, O. (2013). Refining E-government Readiness Index by Cloud Computing. *Jurnal Teknologi* (Sciences and Engineering), 65(1). <https://doi.org/10.11113/jt.v65.1759>
- Mohammed, F., Ibrahim, O., Nilashi, M. & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. *Information Development*, 33(3). <https://doi.org/10.1177/0266666916656033>
- Morris, G. (2007). Master of Business Administration. Retrieved from <http://chesterrep.openrepository.com/cdr/bitstream/10034/84813/4/chapter 3.pdf>
- Morsy, M., Grundy, J., & Müller, I. (2010). An Analysis of the Cloud Computing Security Problem. In *PROC APSEC Cloud Workshop*.
- Mpekoa, N. & Bere, A. (2013). Factors affecting student attitudes towards mobile-voting adoption: a case of a university of technology in South Africa. In *ZA-WWW 2013 Conference*.
- Mpekoa, N. (2017). An Extension and Validation of the Task-Technology Fit: A Case of a Mobile-Phone Voting System. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, pp. 538–546.
- Muller, G. (2006). The present and the future of usable security. Retrieved from [http://ec.europa.eu/information\\_society/istevent/2006/cf/document.cfm?doc\\_id=1954](http://ec.europa.eu/information_society/istevent/2006/cf/document.cfm?doc_id=1954). Date accessed: August 09, 2015.
- Murd. (2016). Ministry of Urban and Rural Development. Retrieved from <http://www.murd.gov.na/objectives>. Date accessed: January 5, 2018.

- Nastasi, B. K., Varjas, K., Sarkar, S. & Jayasena, A. (2004). Participatory model of mental health programming: Lessons learned from work in a developing country. *School Psychology Review*, 27 (2), 260–276.
- NBC Federal Cloud. (2009). Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies - Draft 10.
- Neale, P., Thapa, S., & Boyce, C. (2006). PREPARING A CASE STUDY: A Guide for Designing and Conducting a Case Study for Evaluation Input. 3–14. Retrieved from <http://www.pathfinder.org/publications-tools/pdfs/Preparing-a-Case-Study-A-Guide-for-Designing-and-Conducting-a-Case-Study-for-Evaluation-Input.pdf>. January 5, 2017
- Nghihalwa, E. & Bhunu Shava, F. (2018). An assessment of cloud computing readiness in the Namibian government's Information Technology departments. *2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)*, 92–97. <https://doi.org/10.1109/MELCON.2018.8379074>
- NIST, Badger, L., Bernstein, D., Bohn, R., Vaulx, F. D, Hogan, M. & Leaf, D. (2011). US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft): Useful Information for Cloud Adopters. *Nist Special Publication, II*, 85. <https://doi.org/10.6028/nist.sp.500-293>
- NIST. (2011). NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards. Retrieved from <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:NIST+Cloud+Computing+Reference+Architecture+Recommendations+of+the+National+Institute+of+Standards+and#1>. Date accessed: September 15, 2016.
- Nunamaker, J.F. & Chen, M. (1991). "Systems Development in Information Systems Research," *Journal of Management Information Systems* (7:3), pp 89 - 106.
- Oates, B. J. (2012). *Researching Information Systems and Computing* (2nd ed.). London: Sage Publications.
- Olivier, M.S. (2009). "Information Technology Research: a practical guide for Computer Science and Informatics", 3rd Edition, Van Schaik Publishers, Pretoria.
- OPM. (2016). Office of the Prime Minister. Retrieved from: <http://www.opm.gov.na/web/office-of-the-prime-minister/department-cabinet-secretariat-policy-analysis-and-coordination>. Date accessed: January 5, 2018.
- Pammett, J.H. & Goodman, N. (2013). Consultation and evaluation practices in the implementation of Internet Voting in Canada and Europe. Ottawa: Elections Canada.
- Patton, M.Q. (2001). *Qualitative evaluation and research methods* (3<sup>rd</sup> ed.). Newbury Park, CA: Sage.

- Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Published in Journal of Management Information Systems*, 24(3), 45–78. Retrieved from: [https://wise.vub.ac.be/sites/default/files/thesis\\_info/Design\\_Science\\_Research\\_Methodology\\_2008.pdf](https://wise.vub.ac.be/sites/default/files/thesis_info/Design_Science_Research_Methodology_2008.pdf). Date accessed: March 5, 2018.
- Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2008). A design Science Research Methodology for Information Systems research. *Journal of Management Information Systems*, 24(3), 47-77
- Peffers, K.E.N. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), pp.45–77.
- Petrov, O. (2009). Backgrounder: Financial crisis and cloud computing - Delivering more for less. Demystifying cloud computing as enabler of government transformation, World Bank, Government Transformation Initiative. Retrieved from: <http://www.siteresources.worldbank.org/.../BackgrounderFinancialCrisisCloudComputing.doc>. Date accessed: September 30, 2015.
- Rajkumar, B., James, B. & Andrzej, M. G. (2011). *Cloud Computing: Principles and Paradigms*. Hoboken, New Jersey: John Wiley and Sons.
- Rastogi, R. (2012). Information Security Service Culture – Information Security for End-users. *Journal of Universal Computer Science*, 18(12), 1628–1642.
- Rebollo, O., Mellado, D., Fernandez-Medina, E. & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, 58, 44–57. <https://doi.org/10.1016/j.infsof.2014.10.003>
- Rosenberg, D. (2009). “Supercloud looms for Japanese government,” CNet News, Retrieved May 20, 2016, from [http://news.cnet.com/8301-13846\\_3-10241081-62.html](http://news.cnet.com/8301-13846_3-10241081-62.html)
- Rosenberg, J. (2009). “The Cloud at your service: The when, how and why of enterprise Cloud Computing”, Manning Publications, New York.
- Rossi, M. & Sein, M.K. (2003) "Design research workshop: a proactive research approach," in: 26th Information Systems Research Seminar in Scandinavia, The IRIS Association, Haikko Finland.
- Rowley, J. (2002). Using case studies in research. *Management Research News*, 25(1), 16–27. <https://doi.org/10.1108/01409170210782990>
- Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. (5th ed). England: Pearson.



- Saunders, M., Lewis, P. & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed). Harlow: Pearson
- Schein, E. H. (2004). *Organizational culture and leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.
- Schreier, M. (2012). *Qualitative Content Analysis in Practice*. Sage Publications Ltd.
- Sekaran, U., & Bougie, R. (2009). *Research methods for business: A skill Building Approach*. (5th ed.). UK: John Wiley & Sons.
- Sen, J. (2013). *Security and Privacy Issues in Cloud Computing. Architectures and Protocols for Secure Information Technology*, (iv), 42.
- Services Administration Cloud PMO, G. (2016). *Best Business Practices for U.S. Government Cloud Computing Adoption*. Retrieved from [https://www.gsa.gov/cdnstatic/Best\\_Business\\_Practices\\_for\\_US\\_Government\\_Cloud\\_Adoption.pdf](https://www.gsa.gov/cdnstatic/Best_Business_Practices_for_US_Government_Cloud_Adoption.pdf). Date accessed: September 28, 2017.
- Shackel, B. (2009). Usability–Context, framework, definition, design and evaluation. *Interacting with Computers*, 21(5–6), pp.339–346.
- Sharma, A. (2013). Do We Really Need Traditional Usability Lab for UX Practice? *In A. Sharma, A. Chakrabarti, & R. V. Prakash (Eds.), ICoRD'13: Global Product Development* (pp. 399-409). India: Springer India.
- Shimba, F. (2010). *Cloud Computing: Strategies for Cloud Computing Adoption*. Retrieved from <http://arrow.dit.ie/scschcomdis>. Date accessed: January 15, 2018.
- Silverman, D. (2013). *Doing qualitative research: A practical handbook* (4 Ed.). London, Great Britain: Sage
- Simon, H.A. (1996). *The sciences of the artificial* (3rd ed.). Cambridge: Massachusetts Institute of Technology (MIT) Press.
- Stake, R.E. (1994). *Case Studies. Handbook of qualitative research*. Thousands Oaks, CA: Sage
- Stallings, W., Bauer, M. & Hirsch, E. M. (2013). *COMPUTER SECURITY* (2<sup>nd</sup> ed).
- Steve, K. (2012). "The Future of Authentication", 1540-7993/12, IEEE, pp: 22 – 27.
- Strecker, T.P. (2009). "Govt IT procurement in for shake-up," *The Dominion Post*, Retrieved from: <http://www.stuff.co.nz/technology/2521317/Govt-IT-procurement-in-for-shake-up>. Date accessed: 09 August 2016.
- Stufflebeam, D.L. & Webster, W.J. (2000). An analysis of alternative approaches to evaluation. *In Evaluation models*. Springer, pp. 23–43.



- Takeda, H., Veerkamp, P., Tomiyama, T. & Yoshikawam, H. (1990). "Modeling Design Processes," in: AI Magazine.
- Tornatzky, L. G., Fleischer M. & Chakrabarti, A. K. (1990). "Processes of technological innovation", Lexington Books.
- Tory, M. & Moller, T. (2005). Evaluating visualizations: do expert reviews work. IEEE computer graphics and applications, 25(5), pp.8–11.
- Tripathi, A. & Parihar, B. (2011). "E-governance challenges and cloud benefit", 2011 IEEE International Conference on Computer Science and Automation Engineering, Publisher: IEEE, pp.: 351-354
- Trivedi, K.M. (2013). Cloud Adoption Model for Governments and Large Enterprises. Retrieved from <http://web.mit.edu/smadnick/www/wp/2013-12.pdf>. Date accessed: November 5, 2017.
- Turner, S. (2013). Benefits and risks of cloud computing. *Journal of Technology Research*, 4, 1–7.
- Vaishnavi, V. & Kuechler, B. (2004). Design Science Research in Information Systems Overview of Design Science Research. Ais, p.45.
- Vanderstoep, S.W. & Johnston, D.D. (2009) Research Methods for Everyday Life Blending Qualitative and Quantitative Approaches. Jossey-Bass, San Francisco.
- Vision 2030. (2004). Namibia Vision 2030. Policy Framework for Long-Term National Development Retrieved from: [http://www.npc.gov.na/?wpfb\\_dl=36](http://www.npc.gov.na/?wpfb_dl=36). Date accessed: January 6, 2016.
- Von Roessing, R. M. (2010). The Business Model for Information Security. Rolling Meadows, IL:ISACA. Retrieved from: <http://www.emi-tuv.hu/uploads/images/1337155050732880470219/isaca-bmis-2010.pdf> 221. Date accessed: March 4, 2017.
- Walls, J., Widmeyer, G. & El Sawy, O. (1992). "Building an Information System Design Theory for Vigilant EIS," Information Systems Research (3:1), pp 36-59.
- Weigelt, M. (2009). "Apps.gov: The new look in government procurement," Federal Computer Week. Retrieved from: <http://fcw.com/Articles/2009/09/28/FEAT-Apps.gov-cloud-computing.aspx?p=1>. Date accessed: March 26, 2015.
- Welman, C. & Kruker, F. (1999). Research Methodology for the Business and Administrative Sciences, Cape Town: Oxford University Press.
- Welman, C., Kruger, F., & Mitchell, B. (2005) Research Methodology. New York: Wiley, 45-87

- West, D. M. (2010). Saving Money Through Cloud Computing. *Governance An International Journal Of Policy And Administration*. Retrieved April 5, 2016 from [http://www.brookings.edu/~media/Files/rc/papers/2010/0407\\_cloud\\_computing\\_west/0407\\_cloud\\_computing\\_west.pdf](http://www.brookings.edu/~media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf)
- Williams, M. I. (2006). Making the move to cloud computing. Retrieved from: <https://www.icaew.com/-/media/corporate/archive/files/technical/information-technology/technology/making-the-move-to-cloud-computing.ashx?la=en>. Date accessed: October 5, 2016.
- Wojciech, C. & Sergiusz, S. (2009). "E-Government Based on Cloud Computing and Service-Oriented Architecture" International Conference on Theory and Practice of Electronic Governance. PP. 5-10.
- Wyld, D. C. (2010). The Cloudy Future Of Government IT: Cloud Computing and The Public Sector Around The World. *International Journal of Web & Semantic Technology*, 1(1), 1.
- Xi, L. & Mitrovic, Z. (2014). Readiness Assessment of Cloud-Computing Adoption within a Provincial Government of South Africa. *4th International Conference on Design, Development & Research*, (September 2014).
- Yin, R. K. (2014). The case study methodology. Thousand Oaks, CA: Sage
- Youssef, A. E., & Alageel, M. (2012). A Framework for Secure Cloud Computing, 9(4), 487–500.
- Zachman, J.A. 1987. A framework for information systems architecture. IBM systems journal, 26(3), pp.276–292
- Zhang, Y. & Wildemuth, B. M. (n.d.). Qualitative Analysis of Content. Retrieved January 5, 2018 from [https://www.ischool.utexas.edu/~yanz/Content\\_analysis.pdf](https://www.ischool.utexas.edu/~yanz/Content_analysis.pdf)
- Zucker, D. M. (2009). Teaching research methods in the humanities and social sciences: how to do case study research. *School of Nursing Faculty Publication Series*, 1–17. <https://doi.org/10.1080/07388940701860318>

# APPENDICES

## Appendix A: Permission Letter



**NAMIBIA UNIVERSITY  
OF SCIENCE AND TECHNOLOGY**  
**Faculty of Computing and Informatics**  
Department of Informatics

13 Storch Street  
Private Bag 13388  
Windhoek  
NAMIBIA

T: +264 61 207 2481  
F: +264 61 207 9481  
E: [di@nust.na](mailto:di@nust.na)  
W: [www.nust.na](http://www.nust.na)

Mr P. Van Heerden  
Ministry of Urban and Rural Development  
Private Bag 13289  
Windhoek

11 March 2016

Dear Mr. P. Van Heerden

**Re: Request for Permission to Conduct Research Study**

I am a registered Masters student in the Informatics Department, Faculty of Computing and Informatics at NUST. As part of fulfilling the requirements of the qualification I am required to conduct a research on the topic entitled: "A secure framework for cloud based adoption in Namibian government sector" The objectives are to assess and investigate the benefits and security issues of adopting cloud computing focusing on Infrastructure and Software as a Services technologies in Namibian government and propose a framework for a secure cloud adoption in the government IT department. It is against this background that I am writing to request permission to conduct the research study at Ministry of Urban and Rural Development, Regional Councils and Decentralized OMAs IT division.

All information provided in this study will be kept confidential and only be used for the purpose of the study. When publishing for the degree, no sensitive information will be disclosed and no direct links will be made to the respondents or actual departments. A report on the research findings will be submitted to your office in detail.

I am looking forward to a favourable response to conducting the research study as mentioned above. If you require any further information, please do not hesitate to contact me on +264 813173537, email [enjunice12@gmail.com](mailto:enjunice12@gmail.com). Thank you for your consideration in this matter.

Yours sincerely,

Eunike Nghihalwa

## Appendix B: Approval Letter



REPUBLIC OF NAMIBIA  
OFFICE OF THE PRIME MINISTER

26 March 2016

### Ref: Research site Approval

To whom it may concern

This letter serves to acknowledge that we have received and reviewed a request by Eunike Nghihalwa to conduct a survey in fulfillment of her research project entitled “**A secure framework for cloud based adoption in Namibian government sector**” at Office of the Prime Minister and I approve of this research to be conducted at our IT department.

In return Ms Nghihalwa will share her findings with us and this will improve our planning for embracing cloud services in our department. Please provide her with the required support and necessary assistance for the successful execution of this study. If you have any questions, please do not hesitate to contact the undersigned.

Yours Sincerely,

*Erastus Amutenya*

Deputy Director: IT

Email: [erastus.amutenya@opm.gov.na](mailto:erastus.amutenya@opm.gov.na)

## Appendix C: Cover Letter



**NAMIBIA UNIVERSITY  
OF SCIENCE AND TECHNOLOGY**

**Faculty of Computing and Informatics**

Department of Informatics

13 Storch Street  
Private Bag 13388  
Windhoek  
NAMIBIA

T: +264 61 207 2481  
F: +264 61 207 9481  
E: [di@nust.na](mailto:di@nust.na)  
W: [www.nust.na](http://www.nust.na)

03 May 2016

To: OPM IT staff  
MURD IT staff  
All Regional IT officers

Dear Participant

**RE: Participation to a research survey: A secure framework for cloud based adoption in Namibian government sector**

You are selected to participate in the study for the dissertation research paper carried by Ms Eunice Nghihalwa as a requirement for the fulfillment of a Master degree in Informatics at the Namibian University of Science and Technology.

The aim of the empirical study is to assess and investigate the benefits and security issues of adopting cloud computing in Namibia. The study will further propose a framework for a secure cloud adoption in the government IT departments, specifically on Office of the Prime Minister and Ministry of Urban and Rural Development including Regional Councils as a case study.

You are guaranteed that all information provided in this questionnaire will be kept confidential and only be used for the purpose of the study. The researcher will be held liable for any contrary behavior that might conflict the interest of MURD as an outcome of the study.

The questionnaire consists of four sections that will take you about 15-20 minutes to complete. Kindly answer all questions, as the quality of the outcome will depend on your answers.

Thank you for your contribution!

Yours Sincerely,

A handwritten signature in black ink, appearing to read 'Eunike N. Nghihalwa'.

Eunike N. Nghihalwa



## Appendix D: Publications

# A Secure Cloud Adoption Framework (SCAF) for the Namibian government information technology departments

Eunike Ndambelela Nghihlwa  
Faculty of Computing and Informatics  
Namibia University of Science and Technology  
Windhoek, Namibia  
enjunice12@gmail.com

Fungai Bhunu Shava  
IEEE member  
Namibia University of Science and Technology  
Windhoek, Namibia  
fbshava@nust.na

**Abstract**—Cloud computing has taken over most of the organizations IT departments operations and is making headlines across the globe. Despite cloud computing benefits, security issues and challenges remains a priority concern. The Namibian government is prompt to contemplate solutions that are cost effective and deliver efficient and effective information and communication technology services to her people. This paper presents a Secure Cloud Adoption framework (SCAF) for the Namibian government IT departments, a case study for Office of the Prime Minister and Ministry of Urban and Rural Development IT departments. Design Science Research (DSR) strategy was used to develop the SCAF framework. The framework consists of four components namely: organizational factors, technological enablers, environmental factors and users characteristics. The study reveals that SCAF can safely guide the Namibian government IT departments on how to adopt cloud computing with minimum security risks.

**Keywords**—Cloud Computing, Secure Framework, Security and Privacy, Adoption

## I. INTRODUCTION

Cloud computing is the technology on the rise that offers the service delivery model that satisfies the needs of government administration, offering Information Technology (IT) departments scalability, elasticity, high performance, resilience and security [1]. Reference [1] also demonstrates that the cloud computing model increases the effectiveness and efficiencies of IT services in economy crisis.

Reference [2] define cloud computing as a model for facilitating convenient, readily available access to shared computing resources via the network, the resources are seamlessly available using least effort to control the allocation. Cloud computing can be delivered as Software as a Service, Platform as a Service (PaaS) and Infrastructure as a Service [3] and these models can be access on the Internet when paid for or authorised by cloud service providers. The delivery models can be hosted on four cloud deployment models namely: hybrid, private, public and community deployment models, which describes the scope of services availed to cloud clients [4]. Cloud computing conjointly offers appealing and essential computing characteristics like “on demand self-services, broad network access, resources pooling, rapid elasticity and measured services” [4].

Reference [3], reveals that cloud computing offer to Namibian government IT departments incredible benefits such as improved and maximised service provision, advanced IT infrastructure, information availability, increased storage and performance, reduce IT infrastructure cost, provides flexibility, centralised management, disaster recovery and secure backup systems, however the study [3], also reveal that cloud computing comes with security issues

and challenges affecting cloud computing adoption in IT departments within the Namibian government. The study [3], indicates that majority of the respondents fear the adoption of cloud computing mainly because of security and privacy issues as well as the complexity of the technology. The respondents feared trusting a third party with their confidential data, loss of data, defining appropriate cloud policies and regulations, bandwidth and rapid support from the service providers especially in the remote areas. Finally, based on their study findings [3], concluded that the Namibia government IT departments are aware of the cloud computing technology and shows positive readiness reflection towards cloud adoption.

In their preliminary work [3], [3] assessed the cloud computing readiness in the Namibian government Information Technology departments. In this paper, we extend their previous work by proposing a Secure Cloud Adoption Framework (SCAF) that can safely guide the Namibian government IT departments on how to adopt cloud computing with minimum risks. The study used Design Science Research (DSR) strategy to develop the framework.

In the next sections, we reviewed related frameworks, DSR research strategy, the secure cloud adoption framework, study significance and conclusion will be presented.

## II. RELATED WORK

### A. Frameworks

According to [5], a framework details a comprehensive description structure of how to create, implement and manage a process. Reference [6] added that it is very important to construct a framework as a terms of reference and guidance for the framework design. Frameworks provide understanding, communicate the identified gaps and provide guidelines to the identified problem [7]. This study discusses five existing frameworks that are essential for the implementation of cloud computing adoption.

### B. Existing frameworks

The first framework for secure cloud computing by [4] provides three security components and their mitigations. The three components are:

**Security and privacy requirements:** defines cloud security and privacy needs including authentication, authorization and integrity.

**Attacks and threats:** which warns against cloud threats and attacks.

**Concerns and risks:** focusing on cloud computing threats and concerns [4].

In this study these essential security components that help mitigate the cloud computing deployment security and privacy issues, attacks, concerns and risks were identified as crucial to the success of secure cloud adoption. Along with the framework, [4] presented a generic cloud security model meant to help in achieving cloud computing security and privacy requirements.

Secondly [8], presented a security framework in cloud computing infrastructure. The framework presents three components namely: Technological, Organisational and Environmental (TOE) context that drives organisations to embrace cloud computing. Technological context: speaks to internal and external technologies needed to drive business. Current technologies supporting organizational vision influence adoption of cloud computing as they define the scope of acceptable technological change. Organisational context: means the resources and characteristics of the organisations. It consists of two main components namely top management and technological readiness. Of importance in the adoption of new technologies is senior management buy. Management buy in is usually evidenced in their budgets that put preference in the initiative. For this to be, clear return on investment should be presented to senior management as it is key to organizational change which drives the business vision.

Technological readiness speaks to the preparedness of cloud computing infrastructure and human resources. Environmental context: covers the environment in which the organisation operates. This includes competitors, trade partners, government policy and vendor scarcity [9]. Cloud adoption promotes a competitive environment by industry structure and outperforming other organisations and with overwhelming cloud benefits, the first organisations are expected to derive these benefits in terms of competitive advantages and survival [10]. The TOE framework will be used in this study as an initial guidance to categorise the identified framework components.

Thirdly, the security framework government cloud by [1] was reviewed as it details the set of actions to be followed for the implementation of secure governmental cloud. Firstly [1] defines the responsibilities of each party involved in the implementation of the framework. The roles comprise of cloud owners (the organisation that legally owns the cloud), cloud service provider (Is the organisation that provides cloud services based on Service Level Agreement (SLA)). Cloud customer: Is the organisation using the cloud services provided by cloud service providers through cloud owners. Secondly, the study [1] identified the logic model phases following the PDCA model cycle: Plan, Do, Check and Act to model information security management systems into the governmental clouds.

Fourthly, the Control Framework for Information and Related Technology (COBIT) version 5 by [11] was evaluated. According to [11] COBIT is an IT governance and control framework which avails a toolset for managers to address the control requirements, technical issues and business risks alignment.

Lastly decision framework for cloud computing to assist managers determine which solution fits their organisation by [12] was studied. In this framework the authors recommend decisions in service architecture, system architecture and application architecture as requirements for migrating to the

cloud. Service architecture assesses how the service is provided and the view of the user on the cloud computing; while System architecture assesses the cloud infrastructure issues and the cloud-based applications. On the other hand, application architecture assesses how applications are mapped to the cloud infrastructure. In this study a framework for secure cloud adoption is presented and it is important for decision makers to be well informed, hence the framework will be used in coming up with SCAF.

### III. FRAMEWORK DESIGN

The study used the six steps of design science research (DSR) strategy by [13] to design the proposed framework for a secure cloud adoption (SCAF) for the Namibian government IT departments. As alluded by [3] DSR is a problem-solving strategy aiming at building and evaluating artefacts to address a phenomena, this will be the basis for choosing it as preferred method in this context. Reference [13] added that DSR is very important to information technology systems for evaluation and iteration within research, as it cater for innovative artefacts to solve real-world problems.

The next section will present the application of the 6 steps to design the SCAF.

#### A. PHASE 1: Identify problem and motivate

Reference [13] stresses that DSR addresses or solve a problem in a unique, innovative, effective and efficient ways. Phase one focuses on the identified research problem and value justification of the solution. The artefact and motivation of this phase is **"to propose a secure framework for cloud adoption in the Namibian government IT departments"**.

#### B. PHASE 2: Define objectives of solutions

Reference [13] says that at this stage the study defines the objectives of the solution from the problem definition.

**The main objectives of this study is to propose a Secure Cloud Adoption Framework (SCAF), that safe guide the Namibian government IT departments on how to adopt cloud computing with minimum risks.**

#### C. PHASE 3: Design and develop

Reference [13] describes this stage as designing the development of the desired artefact functionality and architecture. This section, based on the study findings details the framework identified components and the relationship of these components.

a) *Components identification:* The components were extracted from a study by [3] in the same context. The study valued the findings, as the participants' responses are very important sources of theory [6], these theories are real phenomena and inform of the participants' actions, actual beliefs, values and theories [14]. Existing theories and relevant research facilitated the understanding of the technology being studied.

The study has come up with a concise list of components identified as crucial to the framework for the Namibian government to embrace cloud computing. The identified



components from literature review and research findings were integrated and grouped according to the four TOE framework focus areas namely: technological enablers; organisational factors; environmental factors; stakeholder characteristics, as shown in Table I.

Furthermore, the identified components were clustered according to the adoption process explained in the next section of component validation.

*b) Component validation:* Component validation describes the validation of each of the constructs used during the development of the framework [1]. Four steps involved in the cloud computing adoption process were identified, namely the technological availability, awareness, knowledge and skills and lastly the decision making, according. The next section describes the adoption process in the SCAF framework.

- **Technological Availability:** The adoption process starts with the availability of the cloud computing technology [8] in the organisation and, for this study, in government departments. However, the availability of cloud computing technology is influenced by organisational factors, technological

factors [9]; environmental as well as technological users' characteristics. Organisational factors affecting technological availability include resource availability such budgetary provision and governance of such resources in favour of the cloud computing technology. Technological factors are infrastructure compatibility, bandwidth and challenges [3]. Environmental factors are policies, regulations and cloud providers. Technological user characteristics include technology acceptance by the users. Furthermore, the availability of technology is influenced by enabling technological infrastructure that is capable of delivering the necessary cloud services. The study revealed that all sampled government institutions were well equipped with information technology compatible with cloud service provision.

TABLE I. FRAMEWORK COMPONENTS

Components	Sub-components
Organisational factors	Budget
	Needs assessment
	User characteristics
	Executive management buy-in
	ROI (benefits)
	Trust and privacy (information security)
	Governance
Technological enablers	Infrastructure readiness
	Compatibility
	Performance
	Information security
	Service delivery
	Privacy
Environmental	Policies
	Regulations (cloud, trust and privacy)
	Governance
	Cloud providers
User/stakeholder characteristics	Acceptance
	Awareness and knowledge
	Decision making
	Expectations
	Information security (trust)
	Skills
	Motivation

- **Awareness:** Awareness is very important in all aspects affecting cloud computing [3]. For the executive management to buy in and make well-informed decisions, they need to be aware of the technology and decide if its benefits are worth investing in for the Namibian government. Reference [3] shows that IT experts are aware of cloud. Knowing the technology, is also important to study the environment in which cloud operates. By assessing the policies, regulations, service providers, security controls and ensuring that the expectations are met. Organisational factors that are at awareness level are executive management buy-in and benefits presented. Technological enablers ensure that security and privacy requirements and controls are known as presented. Environmental factors ensure that policies and regulations are met. Lastly, user characteristics includes awareness and expectations.
- **Knowledge and skills:** Knowledge and skills are power in adopting cloud. The executing management should know and understand the whole process of cloud adoption to lead and approve the project. This element involves using the skills and knowledge to define proper policies and regulations governing cloud computing. Governance should be practiced. Reference [15] defines governance as a collection of responsibilities and practices exercised by management to supply strategic direction, making certain that objectives are achieved and ascertaining that risks are managed properly.
- **Decision Making:** The study reveals that based on the adoption factors, the decision to adopt cloud paradigm is influenced by the performance or whether the system is delivering service as expected [12]. Security and Privacy plays a vital role on the sensitivity of data and infrastructural protection. The overall decision is made on trust regarding all aspects of cloud adoption. The components of the decision making at the different adopting factors includes information security, return on investment, performance, governance, performance, service delivery and decision in cloud adoption.
- **Security and privacy:** These elements assess the risks associated with security, privacy and other threats and ensures that security measures are in place.



Countermeasures includes trust management, privacy management, accountability, transparency, access control, authentication, authorisation, integrity, non-repudiation, confidentiality, compliance, governance and data center physical security [1].

- **Monitoring, Evaluation, Auditing and continuous support:** Knowledge and skills ensures sustainability of cloud adoption, executive management must provide continuous support throughout to drive the implementation of cloud technology. Performance monitoring, evaluation and auditing must be performed constantly to detect any risk or threats that might occur as stated in the study outcomes. The next section presents the construct of the relationships.

c) **Construct Relationship:** This section presents the relationship of all the constructs involved in developing the framework. Fig. 1. summarises the interrelationships among the constructs.

**Relationship 1 (R1):** The first relationship identified is the relationship between the users' characteristics, technological enablers, organisational factors and environmental factors. These four components influence and enable the decisions to adopt cloud computing technology. Fig.1. shows how this relationship promotes cloud adoption by ensuring that the cloud technology performs, delivery services, lows cost, ensures governmental privacy, trust and to make sure that security (including information security) is always achieved

**Relationship 2 (R2):** The second relationship is between the user characteristics and technological enablers. Users play an important role in influencing any technological initiatives. Based on the new technology available, the organization identifies and assesses organizational needs. The executive management are aware and understand the return on investments (benefits) of cloud-based technology to the business strategy. Once the departmental objectives and expectations are achieved, the technological readiness is assessed. The overall infrastructure is assessed for compatibility of new technology with current infrastructure and if the internet bandwidth will be able to accommodate all users, and data security and privacy measures are considered. Based on trust, performance and service delivery, the executive management buys into the technology's adoption.

**Relationship 3 (R3):** The third relationship is between environmental factors and organisational factors. Governance: the cloud infrastructure requires well defined policies and regulations. And implementing within an organisation with well-defined roles of responsibilities of IT management, business processes and applications helps the organisation to address the areas of regulatory compliances, risk management and align IT strategy with organisational goals.

**Relationship 4 (R4):** The fourth relationship is between organisational factors and cloud adoption. This relationship ensures that IT investments produce business value as well as mitigate the risks and challenges associated with IT. At this stage, the cost of adoption, migration, acquisition, customisation, uncertainty and cost of data confidentiality and availability loss is determined and calculated.

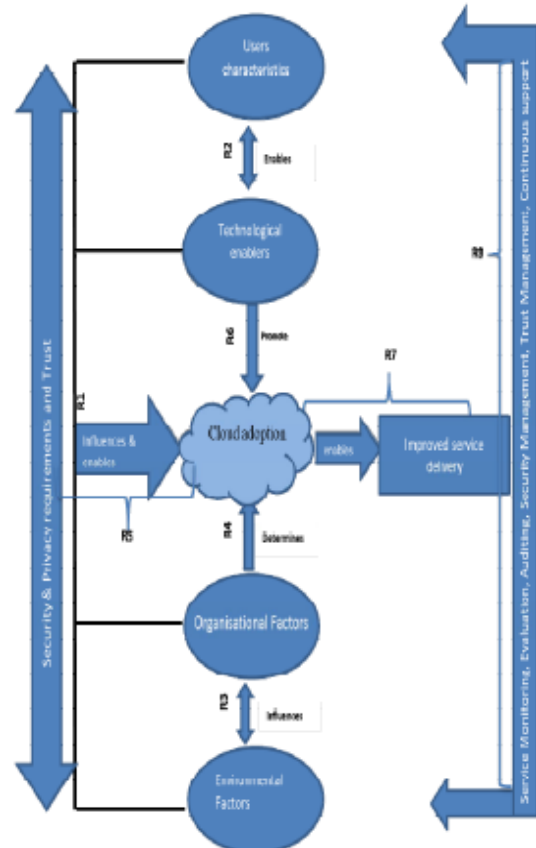


Fig. 1. Construct overall interrelationship

Taking into consideration the overall cost performance required for the adoption of cloud computing in the public sector, the study supports that cloud models are cost-effective but require a huge upfront investment. The top management sums up all cost factors and presents the budget to the finance department in the organisation. The finance department approves and enables the budget.

**Relationship 5 (R5):** The fifth relationship is between adoption factors and security and privacy requirements and trust. The stakeholders ensure that proper security controls that fulfil the security and privacy requirements are in place. The study reveals that cloud computing can only be trusted once proper security mechanisms are in place. This creates a positive working relationship between the cloud owner, cloud customers and cloud providers.

**Relationship 6 (R6):** The sixth relationship is between technological enablers and cloud adoption. Technology enablers promote cloud adoption. This ensures that cloud

adoption is based on the needs and requirements of the government to address the goals and business sustainability.

**Relationship 7 (R7):** The seventh relationship is between cloud adoption and improved service delivery. After the decision to adopt the cloud solution, the next phase is the implementation. Implementation plan and process should be addressed. Implementation is the crucial stage for users to access the cloud services deployed. This ensures that the cloud services to be accessed are available and that all security and privacy requirements are implemented.

**Relationship 8 (R8):** The eighth relationship is between cloud implementation and management (service monitoring, evaluation, auditing, etc). At this stage, it involves governance, which avails an information security consolidated governance, management and process frame. This sums up and covers all the security issues and ensures compliance to all components needed to implement cloud computing.

#### D. PHASE 4: DEMONSTRATION

In this phase, the study demonstrates the application of the artefact to solve the problem.

*a) Stage 1: Identify factors affecting cloud adoption:* The first stage is to identify factors affecting cloud adoption in an organisation. Firstly, the organisational user/stakeholder characteristics involved in cloud computing adoption are defined. The cloud adoption team roles are defined in Table II. The most crucial component is to determine the needs and expectations of the Namibian government IT departments by defining the factors affecting cloud adoption as depicted in Table III.

TABLE II. CLOUD ADOPTION TEAM ROLES

Cloud Computing Adoption Team	Roles	Outputs
Office of the Prime Minister (OPM)	Legally own government cloud	Define policies, select relevant security dimensions and requirements
Directors and deputy directors	Make decisions Assess cloud-based services Approve budget	Influence decision making Identify services to implement on the cloud
Cloud Service Provider Cloud Experts	Provides IaaS and IaaS cloud services and advise accordingly	Deliver cloud computing services
Migration cloud experts Systems administrator System analyst IT technician	Execute the framework	Implement Integrate and migrate to cloud services
Experts review Government employees Internal IT auditors Security experts	Monitor, evaluate and audit the framework	Ensure compliance of policies and security controls Verification of service level agreements
OPM OMA/MURD/RCA/DF	Implementation agencies	Implementations and deployment of the secure framework

TABLE III. FACTORS AFFECTING CLOUD ADOPTION

Organisational Factors	
Needs assessment (Performed by the deputy director, chief system administrator/system analyst, security experts and cloud providers)	Identify services to migrate to the cloud Classification of information asset security categories: official, secret, top secret Determine risk profiling Does cloud computing innovation meet the departmental objectives internal competency skills The departments can sustain themselves IT staff skilled to assist the users
Executive management buy-in (OPM and MURD IT director, deputy director, chief system analyst/system administrator/analyst programmen)	Cloud computing is presented to IT directors, deputy directors and chief system analyst/system administrator/analyst programmen. The executive management understand and grasp the value of the technology Based on strategic planning and decisions making, the management supports the initiative. Motivate for approval and implementation Draft the Service Level Agreement terms and conditions
Expectations (IT technicians and government employees)	This is in line with organisation operations and may include: Reduced IT infrastructure cost Flexibility and scalability Improved service delivery Availability of cloud services to the RCs Well defined security policies Maximize resource utilization Cost effective
Governance (OPM, cloud experts and audit committee)	Strategically align the cloud infrastructure to the Namibian national information technology's mission, needs and goals assuring that the cloud adoption strategy delivers benefits and provides value OPM ensures that resources are available and managed well OPM monitors and measures the progress on the IT departmental performance towards cloud adoption The procurement unit and audit committee ensures that there was transparency in the decision making Ensures that the service provider understand the government strategy
Benefits	Maximise service delivery, reduce cost, increase performance, eliminate lengthy procurement process, increase effectiveness, centralised resources, enhanced information availability, flexibility, disaster recovery, improved storage space, reduction in IT complexities, reduction in IT experts, systems integration, software legacy, auditing, environmental friendliness and the ability to launch rapidly which is a great return on investment to the Namibian government.
Budget (IT directors and deputy directors)	Government cloud computing cost the project and avail budget for cloud computing implementation The budget should include feasibility study cost, initial cloud computing acquisition budget and service level agreement cost
Skills	Cloud Service Providers train the IT staff Conduct training with all users
Privacy and information security (IT directors, deputy directors)	Determine the privacy and security requirements Select relevant security dimensions

and security officer)	(availability, confidentiality, authenticity, privacy, trust management, accountability, transparency and identity management)
<b>Technological Enablers</b>	
Infrastructure readiness (OPM and MURD IT directors, deputy directors, chief system analyst/system administrator/analyst programmers)	Reliable and electricity Internet speed List systems to be rolled over Rollover plan
Infrastructure compatibility (OPM and MURD IT directors, deputy directors, chief system analyst/system administrator/analyst programmers)	Assess the compatibility issues regard to the existing systems and applications
Bandwidth	Upgrade bandwidth at regional councils and constituencies
Security (security experts)	The Namibian government then establishes security requirements. Select relevant security dimensions e.g. availability, integrity, confidentiality, privacy
Service delivery	CSP and implementation team ensures that the cloud system is performing as intent too. Cloud services are reliable and always available
<b>Environmental Factors</b>	
Policies Regulations	OPM in collaboration with other government OMA, draft the recommended policies: cyber security policy, cloud governance policy, IT cloud legislation, cloud implementation guidelines, cloud computing policy, Technology integration policy and cloud security alliance. The implementation team ensures that all laws and regulations related to cloud computing adoption should be adhered too.
Cloud Services Providers (CSP)	The role of the CSP is to advise accordingly. OPM relies on the CSP's experience, skills and the ability to deliver the services. Ensures that services are available to RCs, MURD and DF throughout.
Governance	Compliance of IT cloud legislation and policies Service monitoring and auditing
Information Security	Ensures data security Compliance with all standards Trust and Privacy is maintain through trust management and national data protection laws
<b>User Characteristics</b>	
Acceptance	The users have accepted that cloud computing is useful and easy to use.
Awareness/knowledge	Implement awareness campaigns to capacitate users
Expectations (IT technicians and government employees)	Bringing service closer to the people
Skills	The right skills and knowledge experts are needed for the implementation of cloud adoption. Train IT experts

*b) Stage 2: Establish cloud adoption baseline:* At this stage, the cloud adoption team (deputy directors, chief system administrator/system analyst, system administrator, system analyst, analyst programmer and cloud providers) establish a cloud baseline by ensuring that all activities required in stage 1 are analysed, completed and improve gap identified.

*c) Stage 3: Implementation:* This stage utilises the evaluation results. The technology intervention is being implemented. The organisations are made aware and best practices are in place. An example of the cloud implementation is illustrated in Fig. 2.

*d) Stage 4: Evaluating:* The cloud adoption framework is evaluated after the implementation.

*e) Stage 5: Monitoring, auditing, security management and continuous support:* Monitoring activities involves monitoring the network traffic between sites, systems monitoring, third party equipment, real time monitoring, web applications, operational and administrative. Auditing activities involves internal and external audits. The Service Level Agreement should be updated if there is any change, violations or a renegotiation in terms of system requirement. Security controls should be managed at all levels. Cloud Service Provider should provide continuous support based on the SLA agreement. A clause should be included in the SLA related to finalisation of the contract with the service provider in case the government wants to terminate the contract.

#### E. PHASE 5: Framework evaluation

Each component of the framework is evaluated and validated by the experts. The framework was refined based on the expert reviewer's comments. The study reveals that SCAF is efficient, operational, relevant, useful, adaptable and valuable.

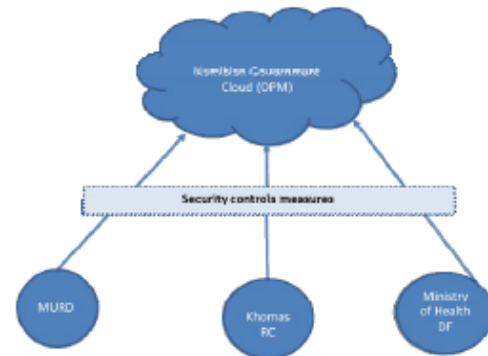


Fig. 2. Namibia Cloud Implementation illustration



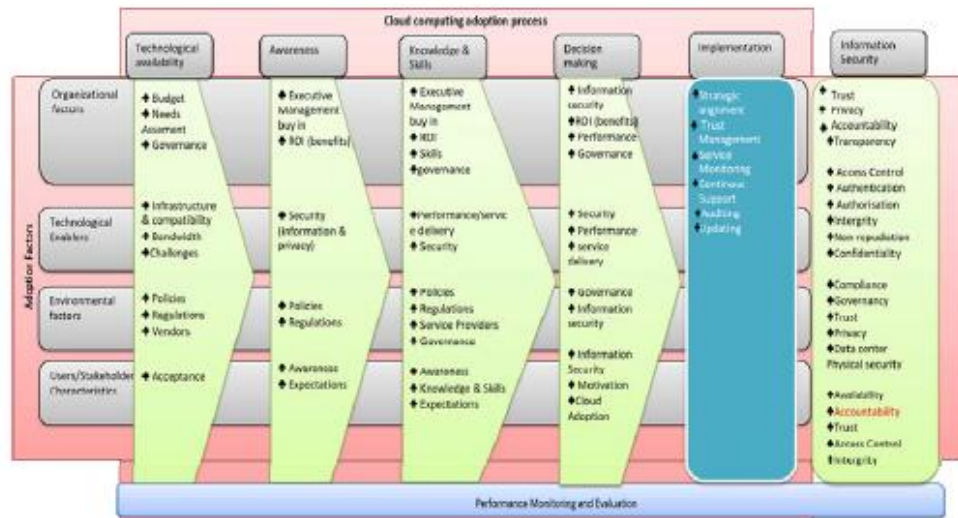


Fig. 3. Secure Cloud Adoption Framework (SCAF)

#### F. PHASE 6: Communication

Fig. 3. Presents the final product of the design, the Secure Cloud Adoption Framework (SCAF). The contributions of this framework will be presented in disseminated peer reviewed scholarly publications such as this one and submitted to the Namibian government IT departments.

SCAF cloud security policy, cyber security policy and cloud adoption strategy needs to be crafted.

In future, the study would present the evaluation and validation results of each SCAF component. Future work also entails generalising the framework to all Namibian government IT departments. The proposed SCAF is flexible for extension and revision to adapt to any cloud security requirements that may arise. The framework can be adopted in similar contexts.

#### IV. STUDY SIGNIFICANCE

The SCAF framework will promote central resource management within the Namibian government IT departments, this will reduce the costs of IT hardware infrastructure, travelling and operations. The SCAF framework can be used as a guide for migrating government traditional wired infrastructural to cloud infrastructural service. The secure cloud adoption framework will assist directors and deputy directors of Namibia government IT departments with decision making and directives on whether to consider adopting cloud for the effective use of technology.

#### V. CONCLUSION

In this paper we presented the proposed secure cloud adoption framework for the Namibia government IT departments. The study reveals that the SCAF is valid and essential for the Namibia government IT departments. The study also reveals that cloud computing offers government IT departments benefits such as cost reduction, flexibility, centralised resources, IT efficiency, improved service delivery, hardware utilisation, data recovery, secure backups, advanced IT infrastructure, increased performance, availability of information and scalability. The Namibian government IT departments can benefit from the mentioned benefits. The study recommends that before implementing

#### REFERENCES

- [1] ENISA. (2015). Security Framework for Governmental Clouds. <https://doi.org/10.2824/57349>
- [2] Mell, P. & Grance, T. (2009). 'The NIST Definition of Cloud Computing', *Communications of the ACM*, 53(6), 50.
- [3] Nghihahwa, E., & Shava, P. B. (2018). An assessment of cloud computing readiness in the Namibian government's Information Technology departments. 2018 19th IEEE Mediterranean Electrotechnical Conference (MELCON), 92-97. <https://doi.org/10.1109/MELCON.2018.8379074>
- [4] Youssef, A. E., & Alaguel, M. (2012). A Framework for Secure Cloud Computing, 9(4), 487-500.
- [5] Roessing, R. M. (2010). The Business Model for Information Security. Rolling Meadows, IL:ISACA. Retrieved March 4, 2017, from <http://www.emi-nv.hu/uploads/images/1337155050732880470219/isaca-bmis-2010.pdf> 221
- [6] Mpekou, N. & Bere, A. (2013). Factors affecting student attitudes towards mobile-voting adoption: a case of a university of technology in South Africa. In ZA-WWW 2013 Conference.
- [7] Zachman, J.A. 1987. A framework for information systems architecture. *IBM systems journal*, 26(3), pp.276-292
- [8] Harfoushi, O., Akhomhaideh, A. H., Aggad, N., Janini, M. A. & Obiedat, R. (2016). Factors Affecting the Intention of Adopting Cloud Computing in Jordanian Hospitals, 9(8), 88-101. <https://doi.org/10.4236/ojs.2016.82010>
- [9] Awad, M. & Leiss, E.L. (2015). Paper Records and Electronic Audits. *Journal of eDemocracy & Open Government (JeDEM)*, 2(1), pp.69-78.

- [10] Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, 28(1). <https://doi.org/10.1108/JEIM-08-2013-0065>
- [11] ISACA (2010) COBIT Framework for IT Governance and Control; ISACA, Retrieved 25 September 2017 from <http://www.isaca.org/Knowledge-Center/COBIT/pages/Overview.aspx>
- [12] Kaisler, S., Money, W. H., & Cohen, S. J. (2012). A Decision Framework for Cloud Computing. <https://doi.org/10.1109/HICSS.2012.52>
- [13] Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems, 22, 9–23. <https://doi.org/10.1007/978-1-4419-5653-8>
- [14] Maxwell, J.A. 2012. *Qualitative research design: An interactive approach: An interactive approach*, Sage.
- [15] ISACA. (2011). introduction to the business model for information security. Rolling Meadows, IL:ISACA. Retrieved February 13, 2017 from [http://www.isaca.org/knowledge-center/research/documents/introduction-to-the-business-model-for-information-security\\_res\\_eng\\_0109.pdf](http://www.isaca.org/knowledge-center/research/documents/introduction-to-the-business-model-for-information-security_res_eng_0109.pdf)

# An assessment of cloud computing readiness in the Namibian government's Information Technology departments

Eunike Nghihalwa  
Faculty of Computing and Informatics  
Namibia University of Science and Technology  
Windhoek, Namibia  
enjunicel2@gmail.com

Fungai Bhunu Shava, IEEE member  
fbshava@nust.na

**Abstract** - Cloud computing is becoming a popular solution for business challenges such as the cost of infrastructure and software; accessibility of services and limited storage space; and as such many organisations including the public sector are embracing it the world over. The cloud technology extends existing Information Technology (IT) potentials without incurring much investment costs. Notwithstanding the benefits associated with cloud technology, the paradigm faces challenges mostly related to security issues such as data leakage, data segregation and legal implications. In Namibia, the government in particular, is faced with serious challenges related to the maintenance of IT infrastructures, high support outsourcing costs and tedious infrastructural procurement processes. Studies elsewhere have shown that such challenges can be solved through the adoption of cloud computing. This paper aims to assess the adoption readiness for cloud based services in the Namibian government. The research employed a qualitative research approach using a case study of three government institutions namely: Office of the Prime Minister, Ministry of Urban and Rural Development, and Regional Councils. The study revealed that officials of the Namibian government are ready to adopt cloud computing as they have perceived that cloud computing is beneficial to government productivity. However, the study also revealed that the government officials were skeptical about the adoption of cloud computing due to the perceived challenges mostly linked to security issues. The findings will contribute to Namibia's Vision 2030 that of connecting all citizens by providing services through new technological horizons.

**Keywords** - Cloud computing, government, case study, readiness, adoption

## I. INTRODUCTION

Cloud computing is a new approach that reduces IT complexity by leveraging the efficient pooling of on-demand, self-managed virtual infrastructure, which can be consumed as a service [1]. Cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly

provisioned and released with minimal management effort or service provider interaction" [2]. The technology has three main service delivery models namely: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These services can be hosted on private, community, public or hybrid deployment models [2]. These models are accessible via the internet and they are made available when the user pays for the resources they need [3].

This study focuses more on IaaS and SaaS, because PaaS provides a combination of infrastructure and applications, focusing more on software development processes which hardly happen in government departments. Considering the current needs, the Namibian IT departments are more focused on getting the current setup through working with limited costs and minimum service interruptions. Hence IaaS offers the government the infrastructure while SaaS caters for the applications needed for the crucial operational functions at the departments.

The cloud computing paradigm is on the increase as evidently seen in both the private and public (government) sectors across the globe [3]. Reference [3] demonstrated that the adoption of cloud computing in the government positively and greatly impacts governments in several ways; cloud services improve service delivery at lower costs, optimise resources utilisation and enhance the government's capacity to develop innovative ideas in order to serve the nation. Government institutions are normally scrutinised over service delivery, hamstrung by "legacy systems and inflexible long-term contracts" which result in governments solely relying on service providers and expertise [4]. Cloud computing is believed to simplify this by the rapid deployment of on demand services, scalability of IT resources, cutting of development times and systems integration flexibility.

Across the globe, governments are looking for best technological ways to perform daily activities that are able to improve interactions with citizens through providing efficient and effective services [5]. The use of the latest



technologies fast-track the processing time needed to deliver service to citizens. Cloud computing increases collaboration amongst different organisations within the government, it reduces data redundancy and promotes the effectiveness of the government through tracking and monitoring their plans [6]. As experienced by the governments in countries such as Japan, Australia, Spain, United Kingdom and United states [7], it is evident that the Namibian government's IT departments can equally benefit from the adoption of cloud computing. Namibia's ultimate objective for Vision 2030 aims to improve the quality of lives to the level of other counterparts in the developed world [8], with national development programs and strategies aimed at achieving this objective. One of the Vision 2030's focus themes that is meant to address this objective is having a knowledge based economy and Information Technology (IT). Nowadays Information Technology is the driving factor to development forces and the Namibian government is prompted to consider solutions that are benefiting and adding value to the government [8], limiting budget costs and maximizing the use of government resources such as cloud computing to deliver efficient and effective information communication technology services to its people. Hence this study seeks to identify and assess the readiness of the Namibian government's IT departments to adopt and explore cloud computing. A case study of the Office of the Prime Minister (OPM), hereafter referred to as the governing unit, and Ministry of Urban and Rural Development (MURD) hereafter referred to as Ministry and Regional Councils (RCs) is considered.

#### A. Case study description

Fig. 1 shows the uniqueness of the case study. The governing unit is an institution that enables the Namibian government to operate at developed country level in pursuance of Namibia's Vision 2030 [9]. Its mandate in ICT management is to:

“Provide Service concerning the development and maintenance of up-to-date and viable computer information based on both political and administration matters. To facilitate the processes of the formulation of policy and implementation of programs within the governing unit and the Public Service as a whole, and To provide operational data Service; develop and maintain systems; investigate Offices/Ministries/Agencies’ (OMAs) computer related needs; recommend appropriate systems; control the acquisition of hardware and software in the entire Public Service through the Tender Board; draw up hardware/software specifications for the invitation of tenders and evaluate delivered goods and services” [9].

The case ministry is one of the Ministries that fall under the governing unit. The ministry's mission is the delivery of services to the satisfaction of all communities through rural development, and the establishment of an effective, decentralized Regional and Local Government system, housing and physical planning. The Ministry has the role to coordinate and spearhead the decentralisation process [10].

The ministry offers IT support to fourteen Regional Councils (RC) in all fourteen regions around the country. The Regional councils then technically support the constituency offices and decentralized functions such as those of the Ministry of Education, Ministry of Works and Transport, Ministry of Health and Social Services, and others that still have to be decentralized to the remote areas. The government aims to bring service delivery closer to its people.

In summary, OPM is the leading government agency that approves, oversees and coordinates the implementation of all developmental initiatives of new technologies within the Namibian government's IT infrastructure. Having the OPM implementing cloud computing will put the country at an advanced stage with regards to the use and adoption of cloud computing.

In addition to the OPM, the Ministry (MURD) plays a key role in the use of IT infrastructure in the government of the Republic of Namibia as it is responsible for the coordination of the decentralisation of the government functions and it houses the Regional Councils. In that regard, assessing MURD on the readiness of cloud computing enhances the adoption of cloud computing by the government of Namibia. Like the MURD, the RCs will house all the centralised government functions, hence the use of cloud computing by RCs and decentralising ministries will advance the government's readiness to adopt cloud. RCs are the implementing agents of the government through the Decentralization Policy.

The infrastructure of server rooms in IT departments are characterised by wired networks, servers, storage spaces and virtual machines. The servers and virtual machines are managed by the ministry's IT personnel. The ministry is faced with challenges such as IT infrastructure which are difficult and expensive to maintain, outsourcing of project expertise to private companies, few IT staff members, tedious hardware/software procurement processes, decentralised management and maintenance of IT infrastructure and IT staff members travelling to regional centres to attend to major issues.

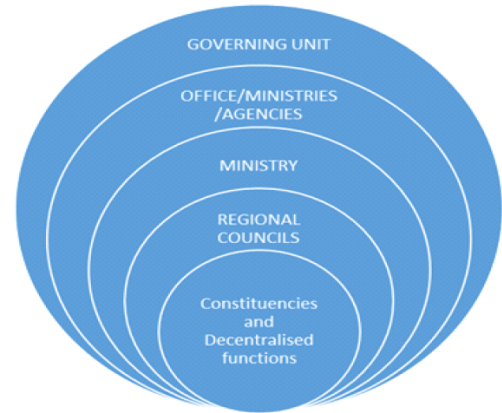


Fig. 1. Case study relationship

the regions, in line with e-government to bring services closer to all the Namibian people. In light of the above, it is assumed that MURD will produce critical information, which is typically significant in achieving the objectives of this study. Reference [15] emphasized that having multiple case strategies strengthens the findings of the entire study because of its presumed replications of the same phenomenon.

#### B. Data Analysis

The collected data was analysed for themes around the benefits of cloud computing and service delivery themes. Emerging patterns were then interpreted using literature and documents in the context. Graphical representations of supporting statistics were generated and they are presented in section IV.

### IV. RESULTS

This section presents the results of the study in four themes namely: i) Characteristics of the informants, ii) Perceived importance of IaaS and SaaS, iii) Challenges hindering the adoption of cloud computing by the Namibian government's IT departments and iv) Service delivery and accessibility.

#### A. Characteristics of the respondents

The respondents of this study were purposively stratified from the Namibian government institutions based on their roles as explained earlier in the case study section. The majority (36%) of the respondents were drawn from the Regional Councils due to their active role regarding the delivery of government services. All Regional Council offices are entrusted with day-to-day administration functions to ensure the delivery of quality services in the regions. The study reveals that IT infrastructures are key to the success of any office administration; hence the study to assess the readiness of how cloud based services as a solution was redeemed necessary, while the governing unit and the ministry accounted for 24% each. The decentralised ministries accounted for the least chunk of the respondents with 16%.

On the other hand, the study was conducted on government officials at technical and managerial levels for Information Technology as presented in Fig. 3. The majority of the respondents comprised of IT System Administrators and Technicians as they make up the large number of supportive staff at all levels. In addition, these System Administrators and Computer Technicians are involved in day-to-day IT support activities and hence their views represent the real-world situations and exhort cloud computing adoption readiness. Other respondents' categories such as senior system administrators and technicians as well as the IT managers also play a crucial role in supervision, decision making and soliciting of IT solutions. Reference [16] developed a decision framework that assists managers to allocate investments and assess cloud alternatives that now compete with in-house data centres.

System Analysts and Programmers are more involved in IT system specifications and solutions. The use of IT experts in providing information on the adoption of cloud computing can generate reliable information as asserted by [17], who stressed

that IT experts' responses confirm the level of reliability of the results and thus provide for good inputs for assessing the readiness of the new technology.

Furthermore, the combinations of various government IT experts in providing information on cloud computing put this study at an advantage as their variety of experiences provide different perspectives of cloud computing understanding. The involvement of these IT experts' portfolios in the use of the cloud paradigm enhances knowledge, expertise and confidence on the influence of cloud adoption in the Namibian government.

#### B. Perceived importance of IaaS and SaaS

While it has been presumed that cloud computing was a new concept in Namibia, the study revealed that the majority of the respondents (76%) were at least familiar with the cloud computing concept. Of the total, 36% of the respondents were very familiar about the cloud computing, 20% were familiar and 20% were relatively familiar. This implies that most of the government officials are knowledgeable and fully aware of the cloud computing concept, they understand the implications of the cloud technology and they are confident to use the technology. However, the study also reveals that 24% of the respondents were just introduced to cloud computing and they are yet to grasp the insights and full understanding of the technology. This high level of understanding cloud computing in the Namibian government puts the country at a reasonable level to adopt cloud computing and hence to benefit from it.

Cloud computing, IaaS and SaaS in particular have numerous significant advantages to any government institutions [3] such as flexibility, cost effectiveness, no upfront payments, IT capacity on demand, increased collaboration, hardware utilisation, centralised IT resources, etc. To assess the readiness of the Namibian government, respondents were asked to express their opinions on how they valued IaaS and SaaS cloud delivery services to the Namibian government's IT departments. The perceived levels of importance are grouped into two categories such as positive perceptions and negative perceptions. Positive perceptions imply that the respondents are in favour of the perceived benefits towards cloud adoption readiness and the positive attributes associated with cloud, while negative perception implies that respondents are unsure of what the technology entails.

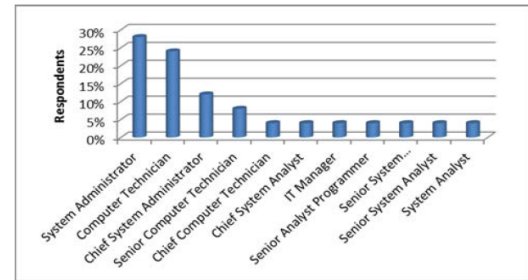


Fig. 3. Portfolios of respondents



In response, the majority of the respondents were positive and in favour of the cloud paradigm, citing that it provides improved service delivery, provides advanced IT infrastructure, avails information, increases performance and storage capacity, saves cost, and provides flexibility and secure backup systems. However, about 3% of the respondents' perceived importance of IaaS and SaaS to Namibia were considered as negative, as the findings revealed that these respondents were unsure of the uncertainties that the cloud technology entails. This might be that these respondents had just learnt about cloud computing as stated earlier. Details of the respondents' perceptions are presented in Fig. 4. The findings are supported by other authors such as [3] and [8], hence there is a positive influence on the readiness of the Namibian government's IT departments.

#### C. Challenges hindering the adoption of cloud computing by Namibian government IT departments

As experienced elsewhere [3], the adoption of cloud computing in Namibia is also not free from the cloud paradigm technological challenges. The results indicate that the majority of the respondents fear the adoption of the technology due to its security and privacy issues (30%) and complexity (23%) of the technology (Fig.5). With regards to security and privacy issues, reference is made to issues such as unnecessary loss of data, accessibility of confidential data by third parties and the challenge of trusting an unknown institution to manage the government's valuable data. This is in line with the findings by other authors such as [2], [18], [19] and [20]. In terms of technology complexity, the respondents are unsure of the availability of the network bandwidth and poor unsupported network infrastructure, especially in the remote areas such as the RCs.

Even though complexity issues have been cited by other authors in relation to the readiness for adopting cloud, authors such as [3] found this challenge to be less important as the availability of internet technology has improved significantly across the globe. Namibia has one of the best internet infrastructure provided by Wax fibre cables that links Africa to European countries. However, the status of localised internet infrastructure may be affected by budget constraints. For instance, the need for improving the internet bandwidth especially in the regions is affected by Namibian's limited budget. Other challenges listed include fear for initial investments costs, limited IT (cloud) knowledge, volume licencing as well as the legal implications such as cloud security policies.

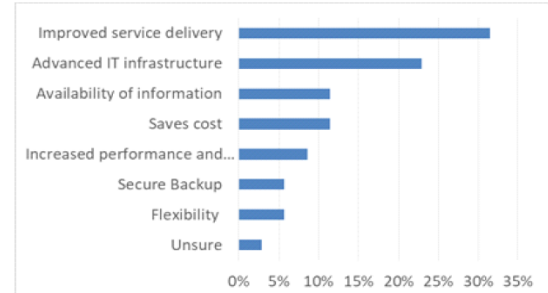


Fig. 4. Perceived importance of IaaS and SaaS to Namibia

#### D. Service delivery and accessibility concerns

Respondents were also asked to list and rate issues affecting IaaS and SaaS service delivery and accessibility. All the respondents cited the availability of the vendor's commitment as the main concerns affecting service delivery and accessibility. About 96 % of the respondents indicated lack of expertise as the second main concern, and this can cripple the adoption. Other areas of concern regarding service delivery and accessibility include bandwidth and service availability and other minor issues. Respondents were further asked whether the adoption of cloud infrastructure and software as services will maximise service delivery in IT and solve backlog problems such as asset underutilisation, hardware failures, lengthy procurement processes and travelling long distances to solve problems and any other IT related problems.

All participants (100%) were in agreement that cloud infrastructure and software as services will maximise service delivery and solve backlog problems, citing that it comes with the following benefits: service availability, reduces IT infrastructure costs, and provides secure data recovery setup, backup and disaster recovery, and ability to solve problems on the click. Hardware failures are easily detected, high adoption, and applications available everywhere and anytime. There are also no license fees (SaaS subscription based), as well as the advantage flexibility and centralized management.

#### V. STUDY SIGNIFICANCE

The research contributes to capacity building as it can be used as a reference material for migrating the government's traditional wired infrastructure to cloud Infrastructural service. To ensure transferability of the study to similar contexts, a research audit trail was maintained and it will be published as part of a Master's thesis. Cloud increases productivity, efficiency and cost reduction. It will also contribute to the knowledge base on the adoption of cloud computing services in Namibia's government IT departments and the security risks that are involved. Moreover, it will assist with informed decision making and directives to adopt cloud technologies, and most significantly it provides guidelines on how to improve secure service delivery in the Namibian's government IT departments.

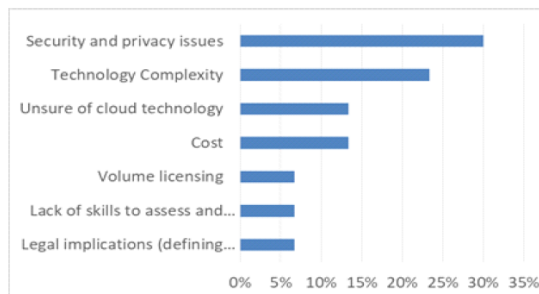


Fig. 5. Challenges hindering cloud adoption

## VI. CONCLUSION

The study concluded that the majority of the Namibian government's IT officials are aware of cloud computing. The cloud computing paradigm offers incredible benefits such as scalability, increase productivity and efficiency. The respondents showed great positivity towards cloud adoption readiness in the Namibian government's IT departments as reflected in the results section. This is a first and important milestone towards addressing the challenges faced by the Namibian government's IT departments.

However, while acknowledging technology's advancement gains, the study indicates that more still needs to be done on the challenges and concerns. Security and privacy issues play an important role in hindering the adoption of cloud services in many instances. In this study, the findings reflect that most respondents fear trusting Namibia's data and information with a third party. Technology complexity, lack of skills and cloud computing uncertainties are also factors challenging the readiness. Legal frameworks such as the cloud security policy and cloud adoption strategy still need to be developed.

Future work entails developing a secure framework on how the Namibian government can position herself to migrate to cloud computing with minimum security risks.

## REFERENCES

- [1] Kuyoro, S. O., Ibiokunle, F. & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks (IJCN)*, (Vol: 3)
- [2] Mell, P. & Grance, T. (2009, July 10). Effectively and Securely Using the Cloud Computing Paradigm. NIST. Information Technology Laboratory Retrieved from [http://www.nist.gov/public\\_affairs/contact.htm](http://www.nist.gov/public_affairs/contact.htm)
- [3] Xi, L. & Mitrovic, Z., (2014). Readiness Assessment of Cloud-Computing Adoption within a Provincial Government of South Africa. 4th International Conference on Design, Development & Research. (September 2014).
- [4] Assessment, C.R., (2010). Cloud Readiness Assessment. , 44(0), pp.6–7.
- [5] Layne, K. & Lee, J., (2001). Developing a fully functional e-government: a four stage model. *Government Information Quarterly*, 18, pp.122–136.
- [6] Hashemi, S., Monfaredi, K. & Masdari, M., (2013). Using Cloud Computing for E-Government: Challenges and Benefits. *International journal of computer, information science and engineering*, 7(9), pp.579–586.
- [7] Wyld, D.C., (2010). The Cloudy Future Of Government IT: Cloud Computing and The Public Sector Around The World. *International Journal of Web & Semantic Technology*, 1(1), p.1.
- [8] Vision 2030. (2004). Namibia Vision 2030. Policy Framework for Long-Term National Development Retrieved from: [http://www.npc.gov.na/?wpfb\\_dl=36](http://www.npc.gov.na/?wpfb_dl=36)
- [9] OPM. (2016). Office of the Prime Minister. Retrieved from <http://www.opm.gov.na/web/office-of-the-prime-minister/department-cabinet-secretariat-policy-analysis-and-coordination>
- [10] Murd. (2016). Ministry of Urban and Rural Development. Retrieved from <http://www.murd.gov.na/objectives>
- [11] Bryman, A. (2012). *Social Research Methods* (4 ed.). New York, United States: Oxford University Press.
- [12] Silverman, D. (2013). *Doing qualitative research: A practical handbook* (4 ed.). London, Great Britain: Sage
- [13] Saunders, M., Lewis, P., & Adrian Thornhill. (2009). *Research Methods for Business Students*. 5th . England: Pearson Education Limited.
- [14] Creswel, J. W. (2008). The Selection of a Research Approach. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 3–22. <https://doi.org/45593:01>
- [15] Yin, R. K. (2004). *The case study methodology*. Thousand Oaks, CA: Sage
- [16] Kaisler, S., Money, W. H., & Cohen, S. J. (2012). A Decision Framework for Cloud Computing. <https://doi.org/10.1109/HICSS.2012.52>
- [17] Shimba. (2010). Moving online: K-12 distance learning market forecast. Rockville, Simba Information
- [18] Morsy, M., Grundy, J., & Müller, I. (2010). An Analysis of the Cloud Computing Security Problem. In *PROC APSEC Cloud Workshop*.
- [19] Sen, J., 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology*, (iv), p.42.
- [20] Brodtkin, J (2008). Gartner: Seven cloud-computing security risks. IDG Communications, Inc.

## Appendix E: Questionnaire

I've invited you to fill out a form:

### A secure framework for cloud based adoption in the Namibian government sector

This study is prepared to assess and investigate the benefits and security issues of adopting cloud based Infrastructure as a Service (IaaS) and Software as a Service (SaaS) technologies and propose a framework for secure cloud adoption in the Namibian government IT departments. The results will contribute to the guidelines and knowledge based literature on the adoption of cloud computing services in Namibian government IT departments. Your response are crucial in informing the design of a user centric solution. All your responses will be treated in a confidential manner; hence you are requested to provide genuine responses. No reference will be made to the respondent or link to your department on reporting. All the collected information will be used for purposes of this study only. Thank you for your time and cooperation!

#### Section A : General Questions

Answer the following questions accordingly:

**1. From which of the following Namibian government IT departments do you belong too?**

For Regional Councils and Decentralised OMA, please specify on other, the name of your RC or Decentralised OMA.

- ☐ Office of the Prime Minister
- ☐ Ministry of Urban and Rural Development
- ☐ Regional Council:
- ☐ Decentralised Function/OMA:
- ☐ Other:

**2. Which of the following best describes your IT job role in the Namibian government?**

**3. To what extent are you familiar with the concept cloud computing?**

- ☐ I am not familiar at all
- ☐ I am just beginning to familiarise myself
- ☐ I am relatively familiar
- ☐ I am familiar
- ☐ I am very familiar

**4. In your own opinion, what could IaaS and SaaS cloud deploying services primarily mean to the Namibian government IT departments?**

Continue »

## SECTION B: CLOUD BENEFITS

Answer the following questions by selecting your preferred correct answer and on the spaces provided:

5. In your own opinion, what benefits does cloud computing (IaaS and SaaS) have over the current traditional IT infrastructure?

Your answer

6. How would you rank in order of importance the following benefits of cloud computing to OPM/MURD/RCs/Decentralised Functions OMAs?

	Not important at all	Slightly important	Important	Very important	Extremely important
Increased collaboration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pricing flexibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No upfront	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Convenience for the development teams	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT efficiency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability to grow and shrink	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT capacity on demand	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability to rapidly launch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
New products and services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Operational cost savings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software cost savings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hardware utilisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improved security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Better functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Complexity reduction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Better scalability and more flexibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Ability to rapidly launch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
New products and services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Operational cost savings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software cost savings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hardware utilisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improved security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Better functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Complexity reduction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Better scalability and more flexibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralised IT resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

BACK

NEXT

Page 2 of 3

## SECTION C: Security challenges and other related issues

Answer the following questions accordingly:

7. What do you think will be the main challenges for Namibian government IT not to consider cloud computing?

Your answer

8. What are your main concerns regarding the use of cloud computing?

- ☐ Security issues
- ☐ Legal issues
- ☐ Compliance issues
- ☐ Privacy issues
- ☐ Integration issues
- ☐ Insufficient financial benefits
- ☐ Lack of functionalities
- ☐ Lack of performances

☐ Immature technology

☐ Loss of data control

☐ Other: \_\_\_\_\_

**9. Which of the following will be the main concern for the OMA, RCs and Decentralised function to access IaaS and SaaS delivery services?**

☐ Bandwidth Capacity

☐ Lack of expertise

☐ service availability

☐ Insufficient vendor service commitment

☐ Other: \_\_\_\_\_

**10. Statement: Security concerns are blocking issues when it comes to cloud computing.**

☐ Strongly Agree

☐ Agree

☐ Undecided

☐ Disagree

☐ Strongly disagree

BACK

SUBMIT

Page 3 of 3

## **Appendix F: Interview**



**NAMIBIA UNIVERSITY  
OF SCIENCE AND TECHNOLOGY**

**Faculty of Computing and Informatics**

**Department of Informatics**

### **A secure framework for cloud based adoption in the Namibian government sector Interview Questions**

---

The objective of this interview is to find out what are the security issues and challenges in adopting cloud based Infrastructure as a Service and Software as a Service in Namibian government institutions?

---

1. Do you think the adoption of cloud infrastructure and software as a service will maximise service delivery in IT and solve backlog problems such as asset underutilisation, hardware failures, lengthy and travel long distance to solve problems and any other IT related problems?
2. What do you think will be the main cloud challenges in the Namibian IT environment?
3. In Namibia, how would you like your sensitive data to be stored and secured? Can we trust cloud providers with the government's sensitive data?
4. Comparing traditional IT infrastructure to cloud IT infrastructure, what are the security risks?
5. Do you believe that cloud computing Infrastructure is the future IT model for government despite the security challenges involved?
6. What are your recommendation/your input on the Namibian government cloud adoption in the IT department?
7. What IT policies and legalisations do you think are critical for Namibian cloud adoption?
8. If the Namibian government IT departments consider cloud Infrastructure, who should govern it?
  - Congress through legislation
  - Organisation

- **Public coalition**
- **Private coalition**
- **Cyber security**

## **Appendix G: Framework Evaluation tool**

### **A secure framework for a cloud based adoption in the Namibian government sector**

Dear Participants

This questionnaire serves as an evaluation tool for evaluating a secure framework for cloud computing services adoption in the Namibian government sector. Information collected will be used to improve the framework. The resulting framework will contribute to the guidelines and knowledge base on the adoption of cloud computing services in Namibian government IT departments. Your responses are crucial in informing the design of the framework. The study is conducted by Eunike Nghihalwa, under the supervision of Dr Fungai Bhunu Shava from the Namibia University of Science and Technology.

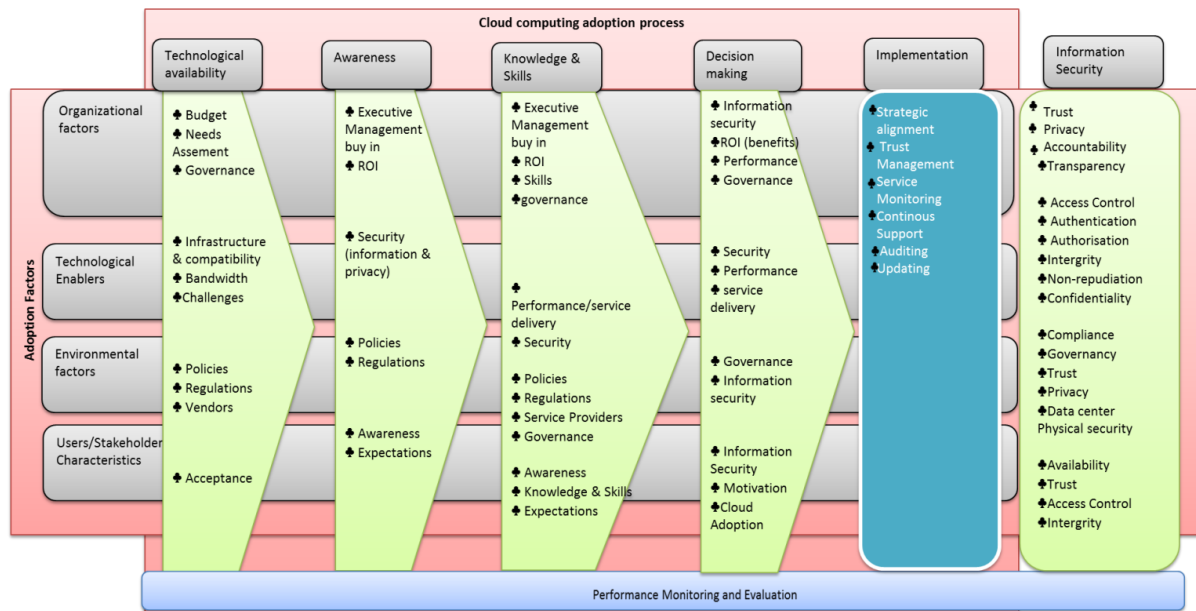
All your responses will be treated in a confidential manner; hence you are invited to provide genuine responses. All the collected information will be used for purposes of this study only. The questionnaire will take about 15-20 minutes of your time. For any further information, kindly contact me on 0813173537 or enjunice12@gmail.com

Thank you for your time and cooperation!



## **Secure Framework for cloud based adoption in Namibia government IT departments**

A framework is defined as an outline of interlinked ideas, which supports an approach to a specific objective that provides a frame of reference that can be modified as and when required (Shackel, 2009; Zachman, 1987). Furthermore, von Roessing (2010) details that frameworks provide a detailed description structure of how to implement, create or manage a programme or process. This questionnaire presents a Secure Cloud Adoption Framework (SCAF) that will inform the Namibian government on how she can securely adopt cloud computing in service delivery.



**Figure 0-1: Secure Cloud Adoption Framework**

## 1. DEMOGRAPHIC INFORMATION

The purpose of this evaluation section is to collect demographic information of different stakeholders to differentiate the selected stakeholders.

Position

- |   |  |
|---|--|
| <input type="checkbox"/> Head of Information Technology | <input type="checkbox"/> IT Technician               |
| <input type="checkbox"/> System Administrator           | <input type="checkbox"/> Information Security Expert |
| <input type="checkbox"/> Internal Auditors              | <input type="checkbox"/> Academic:Prof/Dr./MSc/      |
| <input type="checkbox"/> Security Officers              | <input type="checkbox"/> Analyst Programmer          |
| <input type="checkbox"/> System Analyst                 | <input type="checkbox"/> Others.....                 |

Information Security/Governance Years of Experiences

- ☐ 0 - 5
- ☐ 6 -10
- ☐ 11 - 20+

## 2. FRAMEWORK EVALUATION

### 2.1 NEEDS ASSESSMENT

**How relevant is it to assess the listed organisation's needs in the adoption of cloud computing in the Namibian government?**

Needs assessment	Very Relevant	Relevant	Not Relevant	Least Relevant
The department's IT infrastructure and requirements for the organization's sustainability.				
The mapping of cloud computing adoption to the organisation's strategy, to ensure that the departmental objectives and expectations are achieved.				

Evaluate organisation's internal competency such as skills, management support, availability of infrastructure and resources for cloud adoption.				
The challenges of the existing service delivery framework				

## 2.2 BENEFITS OF CLOUD COMPUTING (RETURN ON INVESTMENT)

**a) How relevant are the listed benefits of cloud computing in influencing the adoption of cloud computing services in the Namibian government?**

Cloud computing benefits	Very Relevant	Relevant	Not Relevant	Least Relevant
Flexibility				
Centralised resources				
Hardware utilisation				
Scalability of IT resources				
Greater IT efficiency and agility				
Cost reduction				
Increased performance and better functionality				
Rapid Elasticity				
Protection, care and technical support				
Auditing and logging				
Reporting and intelligently				
Policies Management				
Systems integration and software legacy				
Business continuity				
Regular backups and disaster recovery				
Maximize improved service delivery				
Accessibility of services				

Improved storage space				
Lengthy procurement process eliminated				
IT experts reduced				
Improved Security				
Enhanced Availability of information				
Environmental friendly				
Reduction in IT Complexities				
Ability to launch rapidly				

**b) To what extent do you agree that the presented benefits are applicable to the Namibian government service delivery?**

Cloud computing benefits	Strongly Agree	Agree	Disagree	Strongly Disagree
Flexibility				
Centralised resources				
Hardware utilisation				
Scalability of IT resources				
Greater IT efficiency and agility				
Cost reduction				
Increased performance and better functionality				
Rapid Elasticity				
Protection, care and technical support				
Auditing and logging				
Reporting and intelligently				
Policies Management				
Systems integration and software legacy				
Business continuity				
Regular backups and disaster recovery				

Maximize improved service delivery				
Accessibility of services				
Improved storage space				
Lengthy procurement process eliminated				
IT experts reduced				
Improved Security				
Enhanced Availability of information				
Environmental friendly				
Reduction in IT Complexities				
Ability to launch rapidly				

### 2.3 CHALLENGES

**How relevant is it to consider the following challenges in influencing of adoption of cloud based Services in Namibian government?**

Challenges affecting the adoption of cloud	Very Relevant	Relevant	Not Relevant	Least Relevant
Security issues				
Privacy issues				
Technology complexity				
Trust of where government data is stored				
Data integrity				
Political interferences				
Compliance issues				
Lack of performance/functionalities				
Lack of skills to assess and implement				
Integration issues				

Inadequate IT budget for volume licensing				
Legal implications				
Insufficient vendor service commitment/lack of expertise				
Limited bandwidth capacity				
Low service availability (Downtime)				
Initial Cost/Budget				
Trust				
Policies to support cloud				
Cloud infrastructure security				

## 2.4 BUDGET

**To what extent do you agree that adopting the Secure Cloud Adoption Framework (SCAF) will reduce the listed costs in the Namibian government IT departments?**

Cloud computing cost effectiveness	Strongly Agree	Agree	Disagree	Strongly Disagree
IT hardware infrastructure and maintenance cost				
Based on SCAF the Namibian government can have a low budget allocated to IT service delivery.				
Travelling costs				
Telephone costs				
Network upgrades cost				
Upfront payment				
Operational cost				
Software cost				

## 2.5 PERFORMANCE

**How relevant are these performance indicators in adopting cloud based services in the Namibian IT departments?**

<b>Technology Performance indicators</b>	<b>Very Relevant</b>	<b>Relevant</b>	<b>Not Relevant</b>	<b>Least Relevant</b>
Scalability				
Reliability				
Service availability				
Bandwidth				

## **2.6 TECHNOLOGY ACCEPTANCE**

**a) To what extent do you agree that the listed Perceived Usefulness factors of SCAF in the Namibian government department service delivery will influence cloud adoption?**

<b>Perceived Usefulness</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Disagree</b>	<b>Strongly Disagree</b>
Improve performance				
Maximise service delivery in government				
High flexibility in delivering services				
Enhanced effectiveness of IT experts on the job				
Meets the Namibian government IT departments needs such as solving backlog issues at the Regional Councils				
SCAF will be useful in supporting Regional Councils and other remote areas				



- b) To what extent do you agree that the Perceived Ease of Use of the secure cloud computing adoption framework in government department service delivery influences cloud adoption?**

Perceived Ease of Use	Strongly Agree	Agree	Disagree	Strongly disagree
Provides easy guidelines for Infrastructure as a Service to be easily integrated with the traditional IT infrastructure				
The Namibian government IT departments would find cloud computing easy to use				
SCAF will enable timeless services				
Stakeholders will have easy access to information and applications				
SCAF is easy to use as a tool for cloud service integration				

## **2.7 INFORMATION SECURITY**

**How relevant are the listed Security controls towards the adoption of cloud based Services in the Namibian government?**

Information Security controls	Very Relevant	Relevant	Not Relevant	Least Relevant
Identification and authentication management				
Authorization and access control				

Confidentiality				
Integrity				
Non-repudiation				
Availability				
Compliance and audit				
Transparency				
Governance				
Accountability				
Trust Management				
Network Security				
Data Center physical security				
Monitoring and evaluation				

## 2.8 POLICIES AND REGULATIONS

**Which policies are important in the adoption of cloud based infrastructure in the Namibian government?**

**IT policies and regulations towards cloud adoption**

The implementation and operation of information security according to organizational policies and procedures.	Very Important	Important	Not Important	Least Important
Cyber security policy				
Cloud governance policy				
IT cloud legislation				
Cloud implementation guidelines				
Cloud computing policy				
Technology integration policy				

Cloud security alliance				
Federal government audit				

## 2.9 GOVERNANCE

**Please rate the importance of listed governance factors in the adoption of cloud based infrastructure in the Namibian government.**

Governance factors (set of responsibilities and practices by executing management in providing strategic direction, ensuring that objectives are met)	Very Important	Important	Not Important	Least Important
Strategic alignment of IT infrastructure to the organization's mission, needs and goals				
Value delivery: assuring that the cloud adoption strategy delivers benefits and provides value				
Resources Management: the availability and management of adequate resources				
Measurement of IT department performance to monitor progress towards cloud adoption				
Compliance of IT cloud legislation and policies				

Identifying controls to mitigate known risks				
Provision of support for efficiencies and continuous improvement				
Transparency in decision making				
Understanding and awareness of cloud computing risks, and effective and appropriate management of these risks.				
Stakeholders trust the government's strategy				
Service monitoring and auditing				

## 2.10 COMPLIANCE

**How important are the listed compliance factors in the cloud adoption in the Namibian government IT departments?**

How important is this compliance factor in cloud adoption?	Very Important	Important	Not Important	Least Important
Identifying local and international laws, regulations and external requirements to be adhered to				
Reviewing and adjusting IT policies, standards and procedures to ensure that legal, regulatory and contractual				

requirements are addressed and communicated				
Monitoring the compliance requirements of IT policies, standards, procedures and regulatory				
IT cloud legislation compliance				

## 2.11 CLOUD ADOPTION

**Evaluate the relevance of technology readiness in the Namibian IT departments?**

How relevant are these factors in adoption of cloud computing?	Very Relevant	Relevant	Not Relevant	Least Relevant
Cloud adoption readiness assessment				
Development of national cloud adoption secure framework				
Service Level Agreement				
Availability of IT infrastructure (compatibility and interoperability)				
Strategic and Operations planning				
Executive Management buy in				
Broadband connectivity/Bandwidth				
Electricity availability and reliability				
Compliance to regulatory requirements and policies				
Information Security				

Implementation budget				
-----------------------	--	--	--	--

## 2.12 OVERALL FRAMEWORK EVALUATION

Please select the option that speaks to your overall performance of the whole framework using the provided measures.

Overall the framework is:	Strongly Agree	Agree	Disagree	Strongly Disagree
Efficient				
Operational				
Well designed and developed				
Relevant and needed				
Useful				
Adaptable				
Requires improvement				
Valuable				

**Any comments:**

.....

**Thank you for your participation**



## Appendix H: Language Editor's Letter

P O Box 55303

Rocky Crest

Windhoek

Namibia

31 July 2018

TO WHOM IT MAY CONCERN

RE: Language Editing

This serves to confirm that I have rendered language editing services to EUNIKE NDAHAMRUELA NGHIHALWA on her research thesis "**A secure framework for cloud-based computing services adoption in the Namibian government sector**".

I have looked at grammar, language, punctuation and sentence flow in preliminary pages and Chapters 1-7 of the document.

Yours sincerely



Nkazana Sarah Mwanandimal

**Sub-Editor, Proofreader**

**Associate Member: Professional Editors' Guild**