A MODEL TO INTEGRATE ICT INTO THE RISK MANAGEMENT PROCESS IN THE PUBLIC SECTOR: THE DEPARTMENT OF WATER AND SANITATION CASE STUDY

by

PHATHISWA BAM

submitted in accordance with the requirements

for the degree of

MASTER OF SCIENCE

in the subject of

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR H ABDULLAH

CO-SUPERVISOR: PROF M MUJINGA

JULY 2023

DECLARATION

Name:	Phathiswa Bam
Student number:	42648084
Degree:	MSc: Computing

A model to integrate ICT into the risk management process in the public sector: The Department of Water and Sanitation case study

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

SIGNATURE

Ms Phathiswa T Bam

DATE: 7 July 2023

DEDICATION

This dissertation is dedicated to my parents, my father, Sandile Bam, and my late mother, Nobandla Bam, for they have instilled in me the principles that shaped and prepared me for this journey.

ACKNOWLEDGEMENTS

This is the most difficult part to write.

I would like to thank GOD for giving me strength from the beginning of this journey until the end. It was not an easy journey, but I made a commitment to reach the destination. To my supervisor (Dr H. Abdullah) and co-supervisor (Prof M. Mujinga), thank you very much for your continued support even when I was ready to give up. I am not forgetting the research and financial support that I received from the UNISA's masters and doctorate programme. Even when we were faced with the pandemic, sufficient resources were made available on various platforms.

To my wonderful daughter, Siwa, I become emotional just thinking about the faith you had in me. The support you gave me while you had your own academics to deal with, only a special kind would do that.

To my amazing sister, Zimkhitha, to give thanks to you is harder. When our mother was very sick, I kept on wondering how I was going to finish this research considering how hectic things were. You made sure that I had extra time to work on my research. Thank you so much.

My dearest mother, Manyawuza, the faith you had in me gave me so much strength during the most difficult time. Even when I had to look after you while you were sick, you still had the strength to remind me that I had work that I needed to finish. You still had the strength to sit next to me while I was working in my room, checking how I was coping with my research. While I had hoped that you would see the outcomes of this research, you departed on 3 September 2021. As difficult as it was, in my heart I committed to finishing this research to honour you. I had to find the inner strength to complete what you were looking forward to seeing.

To the Department of Water and Sanitation and all my colleagues who assisted me by participating in this study, I will always be grateful as this would not have been possible without you. Jolene Schaefer, thank you for your support since the beginning. Lastly, my friends and everyone who supported and cheered me up, I thank God for all of you.

ABSTRACT

Information and Communication Technology (ICT) can be defined as a form of technology that provides access to information through platforms of telecommunication. Risk management is a process of identifying, assessing, and managing the risks within an institution. The purpose of this dissertation was to determine the role played by ICT and how it influenced the effectiveness of risk management in the public sector. The literature review reveals that some of the contributing factors were the availability and access to ICT resources, which result in the organisation's ability to measure the influence of ICT. There were limited studies to prove the impact of ICT in implementing risk management in the public sector. Employing the right approach to integrate ICT into risk management could assist an organisation in managing its risks effectively. The objective of this dissertation was to determine whether the use of ICT to implement risk management has an impact on the effectiveness of risk management. Furthermore, this study intended to propose a model to integrate ICT into risk management processes in the public sector.

A qualitative method using an online survey and a case study using in-depth interviews was followed, in the form of an inductive approach with a cross-sectional time horizon. Data collected were analysed using thematic analysis whereby key themes were identified. The findings indicated that ICT plays a critical role in the effectiveness of risk management. Yet there are various challenges around the use and accessibility of ICT. A formal model to integrate ICT into risk management was proposed for implementation in the public sector. Additionally, this study provided recommendations to address the ICT challenges identified.

Keywords: technology; risk assessments; information technology (IT); IT governance; risk management; information and communication technology (ICT)

PUBLICATION FROM THIS STUDY

Bam, P., Abdullah, H. & Mujinga, M. 2022. Utilizing Information and Communications Technology to enhance risk management, *In 2022 conference on Information Communications Technology and Society (ICTAS)*: 1-6.

LIST OF ACRONYMS

CGICT:	Corporate Governance of Information and Communication Technology
COBIT:	Control Objectives for Information and Related Technologies
COSO:	Committee of Sponsoring Organisations of the Treadway Commission
DEA:	Department of Environmental Affairs
DPSA:	Department of Public Sector Administration
DWS:	Department of Water and Sanitation
ERM:	Enterprise-wide Risk Management
EVA:	Economic Value Added
GRC:	Governance, Risk and Compliance
ICT:	Information and Communication Technology
ISACA:	Information Systems Audit and Control Association
IT:	Information Technology
OHS:	Occupational Health and Safety
PFMA:	Public Finance Management Act
PWC:	Price Waterhouse Coopers
QDA:	Qualitative data analysis
WCG:	Western Cape Government

TABLE OF CONTENTS

DECLARATION i

DEDICATION ii

ACKNOWLEDGEMENTS iii

ABSTRACT iv

PUBLICATION FROM THIS STUDY v

LIST OF ACRONYMS vi

LIST OF TABLES xiii

LIST OF FIGURES xv

LIST OF APPENDICES xvii

CHAPTER 1: INTRODUCTION AND BACKGROUND 1

1.1 INTRODUCTION 2

1.2 BACKGROUND AND MOTIVATION 6

1.3 PROBLEM STATEMENT 10

1.4 RESEARCH QUESTIONS AND OBJECTIVES 11

1.4.1 Main research question (MRQ) 11

1.4.2 Research sub-questions (RSQ) 11

1.4.3 Main research objective (MRO) 12

1.4.4 Research sub-objectives (RSO) 12

1.4.4.1 Research sub-objective 1 12

1.4.4.2 Research sub-objective 2 12

1.4.4.3 Research sub-objective 3 12

1.5 RESEARCH METHODOLOGY 13

1.6 RESEARCH CONTRIBUTION 14

1.7 RESEARCH SCOPE AND LIMITATIONS 14

1.8 DISSERTATION LAYOUT 15

1.9 CONCLUSION 16

CHAPTER 2: LITERATURE REVIEW 18

2.1 INTRODUCTION 19

2.2 LITERATURE REVIEW 19

2.2.1 Risk management in the Public Sector 19

2.2.2 Risk Management During Strategic Planning 20

2.2.3 Information Technology Governance 21

2.2.4 ICT in the Public Sector 23

2.2.5 Use of ICT within Risk Management 24

2.3 ADOPTION OF INTEGRATED RISK MANAGEMENT SYSTEM 26

2.4 OVERVIEW OF THE RELEVANT THEORIES 28

2.4.1 Conceptual Framework for ERM through EVA 29

2.4.2 Diffusion of innovation theory 31

2.4.3 Situational theory 32

2.5 CONCEPTUAL FRAMEWORK 33

2.6 JUSTIFICATION OF THE CONCEPTUAL FRAMEWORK 36

2.7 CONCLUSION 38

CHAPTER 3: RESEARCH METHODOLOGY 39

3.1 INTRODUCTION 40

3.2 RESEARCH DESIGN 40

3.2.1 Research philosophy 42

3.2.2 Research approach 43

3.2.2.1 Deductive 44

3.2.2.2 Inductive 44

3.2.2.3 Abduction.. 45

3.2.3 Methodological choice..45

3.2.3.1 Mono method.. 46

3.2.3.2 Mixed methods 46

3.2.3.3 Multiple methods 47

3.2.3.3.1 Data Triangulation……………………………………………….47

3.2.3.3.2 Investigator triangulation ………………………………………..48

3.2.3.3.3 Theory triangulation ……………………………………………..48

3.2.3.3.4 Methodological triangulation …………………………………..48

3.2.4 Strategy..49

3.2.4.1 Qualitative survey 50

3.2.4.2 Case study.. 50

3.2.5 Time horizon 52

3.2.5.1 Longitudinal 52

3.2.5.2 Cross-sectional.. 52

3.2.6 Data collection 53

3.2.6.1 Survey 55

3.2.6.2 Case study.. 56

3.2.6.3 Instrument development and distribution.............................. 56

3.2.7 Data analysis 57

3.2.7.1 Thematic analysis.. 58

3.3 MEASURING THE TRUSTWORTHINESS OF THE STUDY 59

3.3.1 Credibility 59

3.3.2 Objectivity 59

3.4 ETHICAL CONSIDERATIONS 60

3.5 CONCLUSION 60

CHAPTER 4: DATA COLLECTION AND ANALYSIS 62

4.1 INTRODUCTION 63

4.2 DATA COLLECTION 63

4.2.1 Demographic data for the participants 64

4.2.2 Distribution of the participants..65

4.2.3 Overview of data collection 66

4.2.3.1 Survey 67

4.2.3.2 Case study.. 67

4.3 DATA ANALYSIS.. 67

4.3.1 Familiarisation with collected data 68

4.3.2 Generate initial codes 74

4.3.3 Search for themes..78

3.4 Review themes 81

4.3.5 Define and name themes...83

4.3.6 Present and discuss the results 84

4.3.6.1 Theme 1: Access to ICT tools and resources....................... 85

4.3.6.1.1 Sub-theme 1.1: ICT Tools and resources availability 86

4.3.6.1.2 Sub-theme 1.2: Access and use of ICT resources ………….87

4.3.6.2 Theme 2: Usefulness of the ICT resource ……………………89

4.3.6.2.1 Sub-theme 2.1: Skill competency ……………………………..90

4.3.6.3 Theme 3: Impact of ICT 100

4.3.6.3.1 Sub-theme 3.1: Value of ICT resources …………………….100

4.3.7 Challenges identified by the participants...109

4.3.7.1 Challenge 1: ICT resources 110

4.3.7.2 Challenge 2: Technology and infrastructure 111

4.3.7.3 Challenge 3: Accessibility and reporting 111

4.3.8 Establishing the validity of the findings..115

4.4 INTERPRETATION OF RESEARCH FINDINGS....................................... 116

4.4.1 Theoretical elaboration..116

4.4.2 Conceptual framework 119

4.4.2.1 The factors contributing to the effectiveness of risk management 119

4.4.2.2 How the organisation embraces technology in risk management 119

4.4.2.3 The factors contributing to ICT adoption............................. 120

4.5 DELIVERABLE OF THE STUDY 121

4.5.1 The proposed model to integrate ICT into the risk management process ……………………………………………………………..121

4.5.1.1 Develop a critical list of IT assets 122

4.5.1.2 Threat assessment 124

4.5.1.3 Vulnerability assessment 124

4.5.1.4 Control analysis 124

4.5.1.5 Conduct risk assessment... 125

4.5.1.5.1 Establish context ………………………………………………125

4.5.1.5.2 Risk assessment ………………………………………………125

4.5.1.5.3 Identify, assess, and evaluate risks …………………………126

4.5.1.5.4 Mitigate the risk ………………………………………………..129

4.6 FINAL REMARKS... 134

4.6.1 Emotions that emerged from the interviews and their interpretations 134

4.7 CONCLUSION... 135

CHAPTER 5: RECOMMENDATIONS AND CONCLUSION 136

5.1 INTRODUCTION 137

5.2 ADDRESSING THE RESEARCH QUESTIONS AND OBJECTIVES 137

5.2.1 Research Sub-Question 1 (RSQ 1) and Research Sub-Objective 1 (RSO 1) 139

5.2.2 Research Sub-Question 2 (RSQ 2) and Research Sub-Objective 2 (RSO 2) 139

5.2.3 Research Sub-Question 3 (RSQ 3) and Research Sub-Objective 3 (RSO 3) 140

5.3 SUMMARY OF THE STUDY 141

5.4 RECOMMENDATIONS 142

5.4.1 Use of ICT tools to implement risk management process 143

5.4.2 Fully integrate ICT in all risk management activities to improve the effectiveness of risk management 143

5.4.3 The approach to conducting ICT risk assessment in the organisation 144

5.5 RESEARCH CONTRIBUTION 144

5.6 FUTURE RESEARCH 145

5.7 PERSONAL REFLECTIONS 145

5.8 CONCLUSION 146

REFERENCES 147

APPENDICES 165

LIST OF TABLES

Table 3.1: Research paradigms ... 42

Table 4.1: Distribution of participants ... 65

Table 4.2: Data collection overview ... 66

Table 4.3: Phase 1 – Familiarize with data survey ... 69

Table 4.4: Phase 1 - Familiarise with data – Interviews ... 72

Table 4.5: Phase 2 – Generate initial codes - Survey ... 74

Table 4.6: Phase 2 – Generate initial codes – Interviews ... 76

Table 4.7: Phase 3 – Search themes - Survey ... 78

Table 4.8: Phase 3 - Search for themes – Interviews ... 79

Table 4.9: Phase 4 – Review themes – Survey ... 81

Table 4.10: Phase 4 Review themes – Interviews ... 82

Table 4.11: Thematic Map ... 83

Table 4.12: Summary of the emerged themes ... 84

Table 4.13: Skill competency against ICT ... 90

Table 4.14: Frequency of use ... 97

Table 4.15: Importance and usefulness of ICT resource ... 99

Table 4.16: The impact of ICT in RM ... 101

Table 4.17: Proposed risk mitigations ... 113

Table 4.18: Corrective measures ... 114

Table 4.19: Links - literature and data 117

Table 4.20: Calculation of the asset value 126

Table 4.21: Determining an impact 127

Table 4.22: Determining the likelihood 128

Table 4.23: Risk severity description 129

Table 4.24: Emotions from the interviews 134

Table 5.1: Recommendations 142

LIST OF FIGURES

Figure 1.1: Chapter 1 layout 1

Figure 1.2: The research onion 13

Figure 1.3: Dissertation layout 15

Figure 2.1: Chapter 2 layout 18

Figure 2.2: ERM through EVA 30

Figure 2.3: Conceptual framework 33

Figure 2.4: Technology adoption curve 35

Figure 3.1: Chapter 3 layout 39

Figure 3.2: The Research Onion 41

Figure 3.3: Deductive vs inductive 43

Figure 3.4: Method of collecting data 46

Figure 3.5: Structure and location 54

Figure 4.1: Chapter 4 layout 62

Figure 4.2: Description of participants 64

Figure 4.3: Thematic analysis 68

Figure 4.4: Access to ICT tools and resources 86

Figure 4.5: Self assessed competency level for ND 91

Figure 4.6: Self-assessed competency level for the SAP GRC 92

Figure 4.7: Self-assessed competency level for the IE 94

Figure 4.8: Self-assessed competency level for the Ms Teams 95

Figure 4.9: Self-assessed competency level for the PPT 96

Figure 4.10: Risk assessment process 102

Figure 4.11: ICT corrective measures 109

Figure 4.12: Lack of ICT resources 110

Figure 4.13: Proposed ICT integration risk model 121

Figure 4.14: Response strategies 130

Figure 5.1: Chapter 5 layout.. 136

Figure 5.2: Sub-objective mapping.. 138

LIST OF APPENDICES

Appendix A: Request approval to conduct research.. 165

Appendix B: Approval to conduct research in the Department of Water and Sanitation granted 166

Appendix C: Ethics approval 167

Appendix D: Request for participants 170

Appendix E: Consent form for the participants 174

Appendix F: Questionnaire.. 175

Appendix G Interview questions 184

Appendix H: Interview Schedule.. 186

Appendix I: Raw data from the survey (the spreadsheet captured all the thirty participants – this is an extract) 187

Appendix J.1: Initial coded data from the survey 188

Appendix J.2: Initial coded data from the survey 189

Appendix J.3: Initial coded data from the interviews 190

Appendix K: First level themes - survey 191

Appendix L: Reduced themes - survey 192

Appendix M: Emerged key themes - survey 193

Appendix N: Raw data from the interviews... 194

Appendix O: First level themes - interviews... 195

Appendix P: Reduced themes - interviews... 197

Appendix Q: Emerged Key themes.......... 198

Appendix R: Language Editor’s Letter.......... 199

CHAPTER 1: INTRODUCTION AND BACKGROUND

The introduction and background chapter provides the research with an overview and context to this study based on the research problem the study intended to address. The layout of this chapter is diagrammatically presented in Figure 1.1. This chapter outlines an introduction to the study in Section 1.1, followed by the background and motivation in Section 1.2. Section 1.3 outlines the problem statement with the research questions and objectives in Section 1.4. This is followed by the research methodology in Section 1.5, research contribution in Section 1.6, and research scope and limitations in Section 1.7. Lastly, the layout of the dissertation is presented in Section 1.8 with the conclusion in Section 1.9.

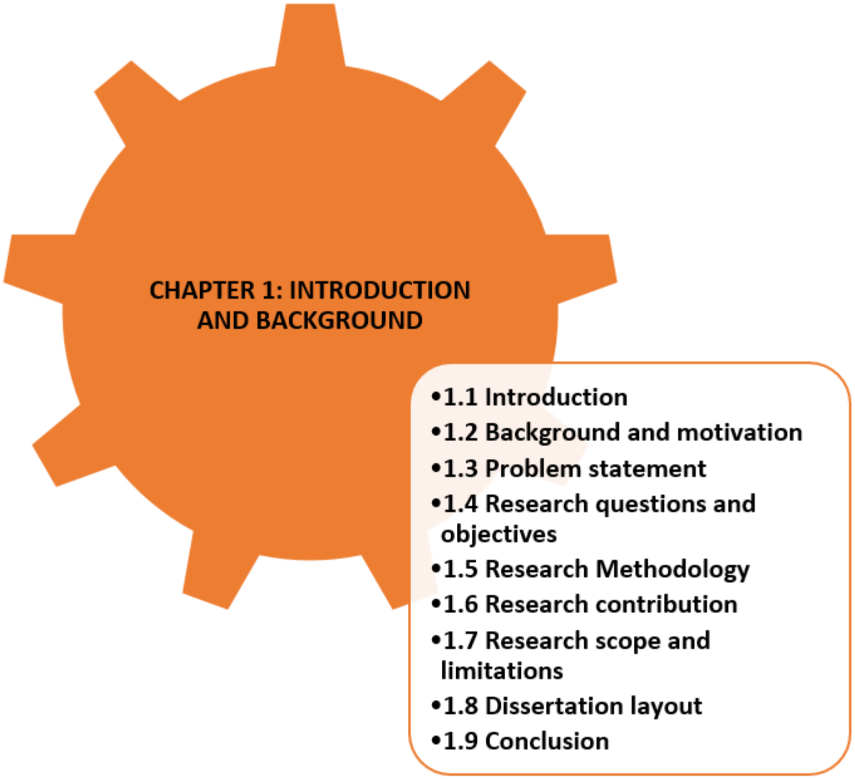

CHAPTER 1: INTRODUCTION AND BACKGROUND
•1.1 Introduction
•1.2 Background and motivation
•1.3 Problem statement
•1.4 Research questions and objectives
•1.5 Research Methodology
•1.6 Research contribution
•1.7 Research scope and limitations
•1.8 Dissertation layout
•1.9 Conclusion

Figure 1.1: Chapter 1 layout

1.1 INTRODUCTION

Risk management is an important aspect for all organisations including the public sector. There are various definitions of risk, yet the key aspect of risk management is managing the effects of uncertainties. International Organisation for Standardization (2018) defines risk as “the effect of uncertainty on objectives” with risk sources, possible events, and their impacts and probability being defined (Institute of Risk Management, 2018, p8). The National Institute of Standards and Technology (2020) views risk as a negative effect from any vulnerabilities that the organisation may be exposed to. Similarly, the National Institute of Standards and Technology (2018) asserts that risk quantifies the extent to which the organisation is exposed to potentially threatening events. Yet de Souza, Braga, da Cunha, and Sales (2020) emphasise that risk should not only be viewed from a negative perspective but from a positive perspective as well, as the risk may trigger opportunities for the organisation. To achieve the objectives of the organisation, the organisation needs to manage the risk(s) (Alijoyo & Norimarna, 2021).

In realising the impact of a crisis, not only financial but also corporate, on business operations, organisations started adopting a comprehensive risk management approach, namely, enterprise risk management (Maruhun, Atan, Yusuf, Rahman & Abdullah, 2021). ISO 31000 defines risk management as the systematic process to guide organisations in managing risk activities. Furthermore, Alijoyo and Norimarna (2021) allude that a risk management framework is provided by the ISO 31000 standards to further support organisations in integrating, designing, implementing, evaluating, and improving risk management processes. To integrate the risk management process in all activities across the organisation, ISO 3100: 2018 standards were issued as an improvement of ISO 31000:2009. The risk management integration intends to avoid the risk management silo approach hence the introduction of Enterprise Risk Management to manage both financial and non-financial risks across the organisation (Saeidi et al., 2021). A wide range of risks affects the operation of all types of organisations, including the public sector (National Institute of Standards and Technology, 2020).

Enterprise risk management guides the organisation in identifying, assessing, and monitoring its risk to ensure the achievement of the objectives across the organisation (Anton & Nucu, 2020). The risk assessments are conducted at all levels of the organisation to determine the link between risk management, organisational strategies, the set objectives, and decision-making. It is important to understand the impact of the risk management process on the organisational objectives. One of the key aspects of risk assessments is to communicate and consult various stakeholders across the organisation. For communication to be effective, the collected information should be efficiently processed and shared with relevant stakeholders (ISO 3100 standards).

Information Communication Technology (ICT) is currently being used to implement risk management in many organisations, both in the private and public sectors (Marx & Shutte, 2018; Khan & Majeed, 2020; Kim & Kim, 2020). ICT "can provide efficient tools for adequate risk management process that would lead to successfully managing and responding to project risks" (Qammaz & AlMaian, 2018, p1). Further, while specific to disaster risk management, ICT has been proven to play a critical role in communicating risk-related information (Ludwig & Mattedi, 2018).

South Africa is a constitutional democracy with a three-tiered system of government and an independent judiciary. The national, provincial, and local levels of government have legislative and executive authority in their spheres. The national government provides laws and policies for the country to abide by and ensure the provision of key services under national competencies. The provincial government administers executive government in the nine provinces. Lastly, the local government administers the supply of goods and services to the citizens.

According to Shand, Parker, Liddle, Spolander, Warwick, and Ainsworth (2022), the public sector exists to provide services to the citizens of the country. The services provided by the public sector include the following (Shand et al., 2022):

- The national and provincial departments focus on the provision of agriculture, health services, housing, tourism, water, disaster management, regional planning and development, trade, and education.
- The local government focuses on municipal planning, municipal public transport, firefighting services, childcare facilities, street trading, and water and sanitation services limited to portable water supply systems and domestic wastewater and sewage-disposal systems.

The main objective of public services is to provide goods and services to the citizens of the country (Eresia-Eke & Soriakumar, 2021). Shipalana (2020) asserts that technological innovation plays a key role in ensuring better service delivery in South Africa. While the public sector institutions are adopting technology, these institutions need to fully embrace innovative strategies by modernising their IT infrastructure (Benbunan-Fich, Desouza & Andersen, 2020). The risk report by the Institute of Risk Management South Africa identified challenges such as infrastructure, high costs, and skills gap as some of the issues affecting delays in embracing technology in the public sector (The Institute of Risk Management South Africa, 2016). Moreover, the Institute of Risk Management South Africa (2021) provided measures to address the digital divide proposing the following:

- Providing access to technology and the internet for the under-resourced areas.
- Providing education and training for the poor.

These measures are intended, among other things, to utilise innovative technologies to build resilience in the public sector. This provides an opportunity to explore the implementation of risk management in government departments focusing on the effects caused by the use of ICT to enhance the effectiveness of risk management. As risk management involves the identification of risks, ICT can assist in collecting data, processing information, and providing tools to report (Qammaz & AlMaian, 2018). Essentially, the use of ICT would ensure the implementation of effective risk management.

Saeidi et al., (2021) associate effective risk management with improved organisation performance in that the process is designed to suit the organisation’s objectives and processes. The implementation of risk management in the public sector is to reinforce the achievement of the sector's objectives. Moreover, having effective risk management will ensure the achievement of the organisation's strategic objectives. Joel and Vyas-Doorgapersad (2019) view risk management as a critical element for effective and efficient service delivery. However, for risk management to have an impact, it needs to be effective. The study conducted by Kong, Lartey, Bah, and Biswas (2018) concluded that failing to monitor the uncertainties in an organisation may result in the objectives not being achieved. For this reason, Tlhogane, Miruka, and Gumede (2018) suggest that the organisation should strengthen their governance structures. Although risk management is deemed to have a positive impact on achieving the organisation's objectives, challenges are prevalent in this area. Furthermore, there are minimal efforts made to understand the effectiveness of risk management in the public sector (Anton & Nucu, 2020).

Numerous studies acknowledged the role played by ICT in risk management (Marx & Schutte, 2018; da Silva Etges & Cortimiglia, 2019; Azizi & Rowlands, 2020). Furthermore, the national integrated ICT White Paper policy recognised ICT to have a critical role in facilitating the objectives of the National Development Plan (Department of Telecommunications and Postal Services, 2016). This policy provides measures to address ICT inclusion in government, such as ICT infrastructure, and ensures access to ICT. This is the reason technology is deemed to play a critical role in implementing effective risk management. The Institute of Risk Management South Africa, 2021) accentuates that the country needs to exploit the opportunities provided by technology. The objective of this study was to investigate the use of ICT to support the implementation of risk management activities in the public sector.

Having provided an overview of risk management, and the value of using technology to support the implementation of risk management, the next section provides the context and the justification for this study.

1.2 BACKGROUND AND MOTIVATION

The risk management process within the public sector is regulated by the Public Finance Management Act (PFMA) of 1999 to ensure that an effective, efficient, and transparent risk management system is maintained within public sector organisations (Department of National Treasury, 2010). As outlined in the Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework, for an organisation to be effective. it needs to achieve its objectives with the resources allocated to it (COSO, 2010). This framework is still relevant and supported by the various pieces of internal organisations' risk management policies that are reviewed frequently.

Joel and Vyas-Doorgapersad (2019) opine that risk management plays an integral part in the strategic management processes during the planning in the public sector. Tworek (2017) concurs with Zainudin, Samad, and Altounjy (2019) who argue that risk management is a critical task that an organisation needs to invest in to achieve its goals. For risk management to add value, Zainudin et al*.,* (2019) emphasise that organisations should manage their human resources as they have a critical role to play in the effectiveness of risk management. As a result, having strong leadership ensures the effective implementation of risk management (Fourie, 2022). This is critical for the organisation as this would entrench risk management in the culture of an organisation and therefore reap the benefits risk management claims to bring. Considering this view, creating a risk-aware culture, especially in the public sector, is vital. Additionally, Saeidi et al., (2021) underscore the importance of risk culture in the organisation. This would be beneficial for the public sector to avoid doing risk management activities for compliance purposes as required by the public sector risk management framework.

According to Nel (2019), the public sector is realising the value of implementing risk management as they acknowledge that the public sector is not immune to risks. ElHaddad, ElHaddad, and Alfadhli (2020) found that there is growth in the implementation of risk management. However, the best practice requires the public sector to create a conducive environment to improve risk management, such as a strong regulatory framework, a risk-aware culture, and senior management embracing risk management with the support of committed risk champions (Nel, 2019). While these appropriate risk management systems promise improvement in risk management, innovative strategies are necessary (Institute of Risk Management South Africa, 2021).

Risk assessments were conducted on various levels, such as strategic and operational, with project risk assessment forming part of the strategic risk assessment (Department of Water and Sanitation, 2021a). It was during these activities that risks were brought to the attention of risk owners to be managed to an acceptable level. To ensure a structured implementation of risk management, the public sector risk management framework was developed and is being implemented (Department of National Treasury, 2010). This framework was developed to operationalise the requirements of the PFMA where the accounting officers are required to maintain effective risk management in their departments, such as the DWS. As stated in the public sector risk management framework, one of the purposes of the framework is to provide support for departments and entities to improve their performance (Department of Public Service Administration, 2010). This is the latest framework developed for the public sector in South Africa. To operationalise the framework, organisations in the public sector developed risk management policies in line with their core business or the mandate of the organisation. The policy provides a guideline on how to implement risk management to add value and to ensure that the strategic objectives documented in the strategic plan are achieved (Water and Sanitation, 2021b).

A strategic plan is a critical aspect that needs to be reviewed to determine how the risk management process is integrated into the planning process. Kanu (2020) defines strategic planning as a process where planning is done to implement the strategy that the organisation has decided upon. During the planning process, targets are set for various business units to ensure that the resources were allocated sufficiently. Ako-Nai and Singh (2019) indicate that where the elements of governance, risk, and compliance are listed, the developed ICT strategy needs to be aligned with the business strategy. This is supported by the Public Service Corporate Governance of Information and Communication Technology Policy Framework (CGICT), where the departments were required to align the ICT strategic goals to the strategic business process (Department of

Public Services Administration, 2012). To operationalise this requirement, an ICT strategy was developed and implemented in line with the latest practices. Canedo, da Costa, de Sousa Junior and Nze (2018, p6) argue that strategic planning in both the public and private sectors “should be complemented by the planning of information systems, knowledge and information”. This raises a critical aspect of whether the risk assessment for the ICT strategy is being conducted, as ICT is an enabler for the organisation.

The Public Sector Information Technology Master Plan is a plan that has been developed to ensure that the strategic goals are achieved (Western Cape Government, 2013). While the master plan was developed in 2013, there are various recent documents supporting the master plan, such as the ICT charter. The DWS also develops its IT master plan in line with the departmental five-year strategic plan. During this planning session, DWS conducts an IT risk assessment for the plan. The identified risks in line with the plan are communicated with the relevant risk owners and monitored on a quarterly basis. This process is also monitored through the Management Performance Assessment Framework and Tool (Department of Planning, Monitoring and Evaluation, 2015). For this plan to add value to the department, all the risks need to be managed (Birkel, Veile, Müller, Hartmann & Voigt, 2019). To realise this, the public sector has established systems in place (both processes and IT systems). These systems include the public sector risk management framework that was developed to guide the public sector department on the implementation of risk management.

During the strategic and annual planning session, IT planning is conducted on a five-year process where risks relating to IT solutions are identified and managed effectively (Department of Forestry, Fisheries and Environmental, 2022). It is important that the department conducts a risk assessment relating to its IT planning and manages them thereafter (Annual Performance Plan 2017/2018 Department of Local Government). The Western Cape Government (WCG) has also developed a strategic ICT framework to ensure the implementation of the CGICT framework within the province. Furthermore, this framework provides the ICT road map that is aligned with the WCG’s strategy. The framework is a phased approach that covers the alignment of ICT with the business strategy and the risk assessment of the ICT resources. To roll out this framework, the ICT plan was developed as well as the risks relating to it, managed and monitored (Western Cape Government, 2013).

Ako-Nai and Singh (2019) argue that, for organisations to implement IT governance effectively, it is important to note the skills of the people involved in implementing IT governance as they have an impact on the implementation. It is also important to note that the literature alludes to the aspect of capacity and skills as the implementation guide of the CGICT has emphasised the importance of having relevant stakeholders who are taking the lead in the implementation of the framework (Department of Public Service Administration, 2014). This may play a critical role in the utilisation of ICT in risk management. While ICT is used throughout the organisation, there may be reluctance in using ICT when considering that the knowledge of IT may be limited (Ako-Nai & Singh, 2019). It is also imperative that literature reveals that the departments like Water and Sanitation, Western Cape Government, and Local Government are indeed implementing IT governance to a certain extent in their organisations (Western Cape Government, 2013; Department of Water and Sanitation, 2021a).

In this study, the researcher suggests that the use of ICT contributes to the effectiveness of risk management in the public sector. This is based on the need to embed the Public Service Corporate Governance of Information and Technology policy framework to address ICT-related risks and experiences that the researcher has as a risk practitioner within the public sector. Furthermore, the researcher forms part of the risk management team that drives the adoption of technology to support the implementation. It is this role that led the researcher to attempt to explore the impact of technology to improve the risk management function.

While risk management was deemed to have a positive impact on achieving the organisation’s objectives, there is insufficient literature on the implementation of risk management in the public sector. Several studies indicate that the use of technology has a critical role to play to support risk management (Zanfei and Seri, 2016; Institute of International Finance and McKinsey & Company (IIF), 2017; Marx & Shutte, 2018). This motivated the need to conduct the study to determine the contribution of using technology to support risk management in the public sector. The next section presents the problem statement derived from the background of the study.

1.3 PROBLEM STATEMENT

Several studies dating back from 2011 were conducted to examine the use and impact of technology in risk management. However, these studies did not address the public sector (Teymouri & Ashoori, 2011; Shutte & Marx, 2014 & 2018; Pattersen, 2015; IIF, 2017). Most of the studies conducted in the public sector focused on the risk management process in general (Kong et al., 2018; Ahmeti & Vladi, 2017; Nel, 2019). It is noted that these studies did not consider the impact of using ICT to implement risk management in the public sector.

The use of ICT in the public sector to support the business operations of the organisation is growing at an extremely fast pace and various challenges and risks affecting the users have been identified. The COVID-19 pandemic has forced the public sector to adopt innovative, effective, and efficient measures to continue delivering services to its citizens. Although integrated risk management is being implemented in various organisations, the effects on the organisation have not been realised (Anton & Nucu, 2020). While several efforts are being made to implement the ICT policy in the public sector, there is no evidence to support how ICT influences the implementation of risk management in the public sector. A gap was identified between the effectiveness of risk management and the use of ICT to support the implementation of risk management in the South African public sector. Some of the key risk management aspects, that the public sector should strengthen, include proper reporting and efficiency of the risk management process (Joel & Vyas-Doorgapersad, 2019).

The problem is that the risk management process has been implemented over the years in the public sector to support the achievement of strategic objectives. Yet risk management is not deemed effective as the public sector does not perceive the impact of risk management on the achievement of strategic goals. While research indicates that there is an integration of ICT in all business processes, there is no explicit evidence that this integration is realised in the risk management processes. In areas where ICT integration is evident in risk management, research does not assure that risk management is effective because of ICT integration. This may result in the public sector not prioritising the ICT strategies to provide reliable and integrated innovative solutions to support the implementation of risk management. Therefore, the research problem for this study is the ineffective implementation of risk management in the public sector. In response to the aforementioned problem statement, research questions and objectives are formulated in the ensuing section to investigate the potential technology model to improve the efficacy of risk management in the public sector. This model will propose a technology-based approach that the public sector should adopt to integrate ICT into risk management.

1.4 RESEARCH QUESTIONS AND OBJECTIVES

This section provides the research questions guiding the research and outlines the research objectives attained at the end of the research.

1.4.1 Main research question (MRQ)

To define and fulfil the objectives of this research, the primary research question is formulated as follows:

MRQ*: How should ICT be used in an organisation so that it has a positive impact on the effectiveness of risk management?*

1.4.2 Research sub-questions (RSQ)

To answer the MQR successfully, the secondary questions are posed as follows:

Research sub-question 1: *How do public sector organisations currently use ICTs to implement risk management processes?*

Research sub-question 2: *How should ICT integration be implemented to contribute towards the effectiveness of the risk management function within the organisation?*

Research sub-question 3: *What techniques are currently being used to conduct technology-related risk assessments?*

1.4.3 Main research objective (MRO)

To fulfil the aim of this research, the primary research objective is defined as follows:

MRO*: To investigate the potential technology model that the organisation ought to adopt to integrate ICT into the risk management process in the public sector.*

1.4.4 Research sub-objectives (RSO)

The MRO is broken down into achievable secondary research sub-objectives (RSO) as follows:

1.4.4.1 Research sub-objective 1

To understand the technological tools utilised to implement risk management. This sub-objective will be explored in Chapter 3 by sub-research question 1.

1.4.4.2 Research sub-objective 2

To determine if the integration of ICT in all risk management activities improves the effectiveness of risk management. This sub-objective will be explored in Chapter 3 by sub-research question 2.

1.4.4.3 Research sub-objective 3

To investigate the methodologies used to conduct ICT risk assessment in the organisation. This sub-objective will be explored in Chapter 3 by sub-research question 3.

1.5 RESEARCH METHODOLOGY

The researcher will conduct this study using the research onion which follows the process of “peeling off” the various layers of the onion (Saunders, Lewis & Thornhill, 2019). As illustrated in Figure 1.2, the various layers of the research onion consist of philosophy, approach, methodological choice, strategy and time horizon, data collection, and data analysis.

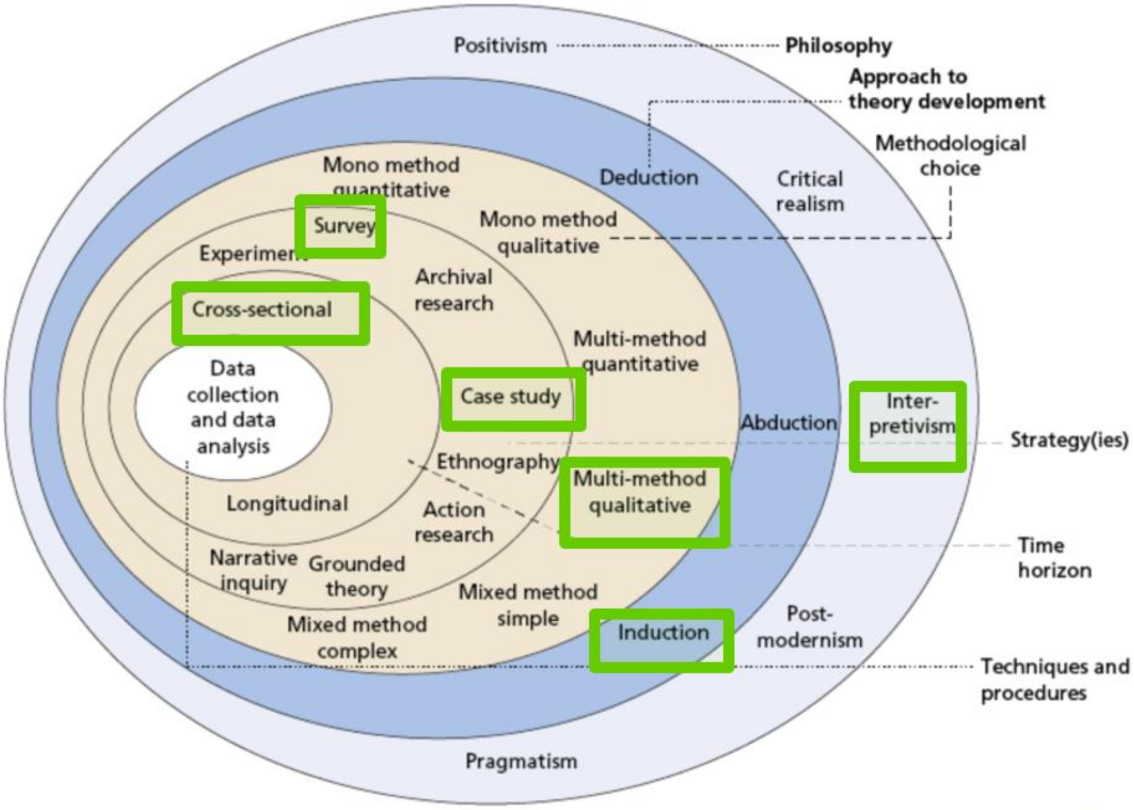


Figure 1.2: The research onion

Source: Saunders, Lewis, and Thornhill (2019)

The study is based on the interpretivism philosophy through an inductive approach with the case study as the research strategy. Data collection will be done over a cross-sectional time horizon, with interviews and a survey conducted to collect data. The collected data will be analysed through thematic analysis. Chapter 3 presents the detailed research methodology.

1.6 RESEARCH CONTRIBUTION

The major contribution of this study is to demonstrate the impact that ICT has on the effectiveness of risk management. The outcomes of the study contribute towards the proposal of the model that integrates ICT into risk management processes within the public sector. By participating in this study, the participants have an opportunity to contribute toward the development of this model. The participants have the added advantage to implement the proposed model and to observe the benefits that the organisation will realise. The proposed model not only assists the department where the research is conducted but all departments in the public sector.

1.7 RESEARCH SCOPE AND LIMITATIONS

This study reviewed the literature that is primarily concerned with the use of ICT to support the implementation of risk management within the public sector. This was done to explore the use of ICT in risk management as well as the influence or effects of ICT to improve the effectiveness of risk management. More importantly, the study provided a strategy to enhance the integration of ICT into risk management activities. This study does not include how the use of ICT in risk management influences the organisation's performance in terms of achieving the planned objectives. A further investigation to determine the impact on the organisational performance may need to be conducted once it is determined that ICT plays a critical role in the effectiveness of risk management in the public sector.

The study is limited to the sampled DWS in the national government where risk management is currently being implemented. The public sector is not only limited to national departments but provincial and local governments as well. For this reason, it may not be possible to implement all the recommendations and the proposed model in all government institutions. The recommendations from this study may need to be customised to fit the structural arrangements of the other government institutions.

The collection of data is only limited to the risk management team and the risk champions in the department as they were mostly involved with daily risk management activities and utilising technology in performing their activities. The risk owners play a key role in risk management and it would have been interesting to get their view on the impact of ICT in supporting risk management. However, the risk owners are not sampled for this study considering time constraints and their availability.

1.8 DISSERTATION LAYOUT

The dissertation structure is outlined in Figure 1.3, providing an overview of the dissertation chapters. Following the depicted structure is the discussion of the contents of each chapter. A similar diagram is presented at the beginning of each chapter.

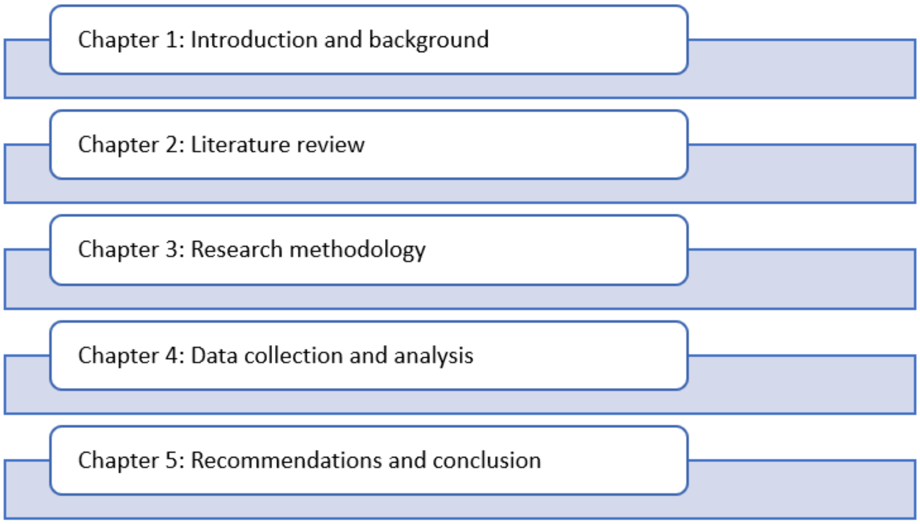

Chapter 1: Introduction and background
Chapter 2: Literature review
Chapter 3: Research methodology
Chapter 4: Data collection and analysis
Chapter 5: Recommendations and conclusion

Figure 1.3: Dissertation layout

Chapter 1: Introduction Background

This chapter provides the introduction and the background information to the study, a statement of the problem, research objective, research questions, research methodology, research contributions, and limitations.

Chapter 2: Literature Review

This chapter provides a detailed literature review regarding the use of ICT to implement risk management and the theoretical background for the study. The three theories, such as the conceptual framework for enterprise risk management through economic value added, diffusion of innovation, and situational theories, are discussed. Furthermore, an overall discussion of the relevant theories is provided with a conceptual framework developed from the existing theories. Finally, the chapter discusses the justification of the study and how the study is viewed through the conceptual model.

Chapter 3: Research Methodology

This chapter provides the methodology adopted while conducting this study, including research design and data collection.

Chapter 4: Data Collection and Analysis

This chapter provides the data collection overview, analysis, and discussions of the research findings based on the data collected. The chapter further proposes a model to integrate technology into risk management.

Chapter 5: Recommendations and Conclusion

This chapter provides the conclusion to the study and provides recommendations for potential future research.

1.9 CONCLUSION

The public sector requires a formal approach to integrate ICT into the implementation of risk management. This chapter provided an overview of the role technology plays to support risk management focusing on integrating ICT into risk management processes in the public sector. This was done to understand whether the risk management process would be effective if technological innovations were integrated. The research gap was identified regarding the use of technology, particularly in risk management in the South African DWS. This led to the desire to pursue the investigation to understand the status of innovation and the impact on the effectiveness of risk management. The fact that various researchers acknowledged the positive impact of ICT in risk management provided further motivation for the study as these studies were not in the public sector.

This will fundamentally contribute to providing a model for the integration of technology in risk management within public sector organisations.

The next chapter reviews the literature to determine the use of ICT to implement risk management activities and determines how the public sector is performing considering that the risk management is implemented in this sector.

CHAPTER 2: LITERATURE REVIEW

The literature review provides an overview of the existing literature relevant to the study, specifically literature with the potential to support the research problem of the study. The layout of this chapter is diagrammatically presented in Figure 2.1. This chapter commences with the introduction in Section 2.1, followed by the literature review in Section 2.2. The adoption of integrated risk management systems is provided in Section 2.3, with Section 2.4 discussing an overview of the relevant theories. The developed conceptual framework is presented in Section 2.5, followed by the justification of the conceptual framework in Section 2.6. Lastly, the conclusion of the chapter is discussed in Section 2.7.

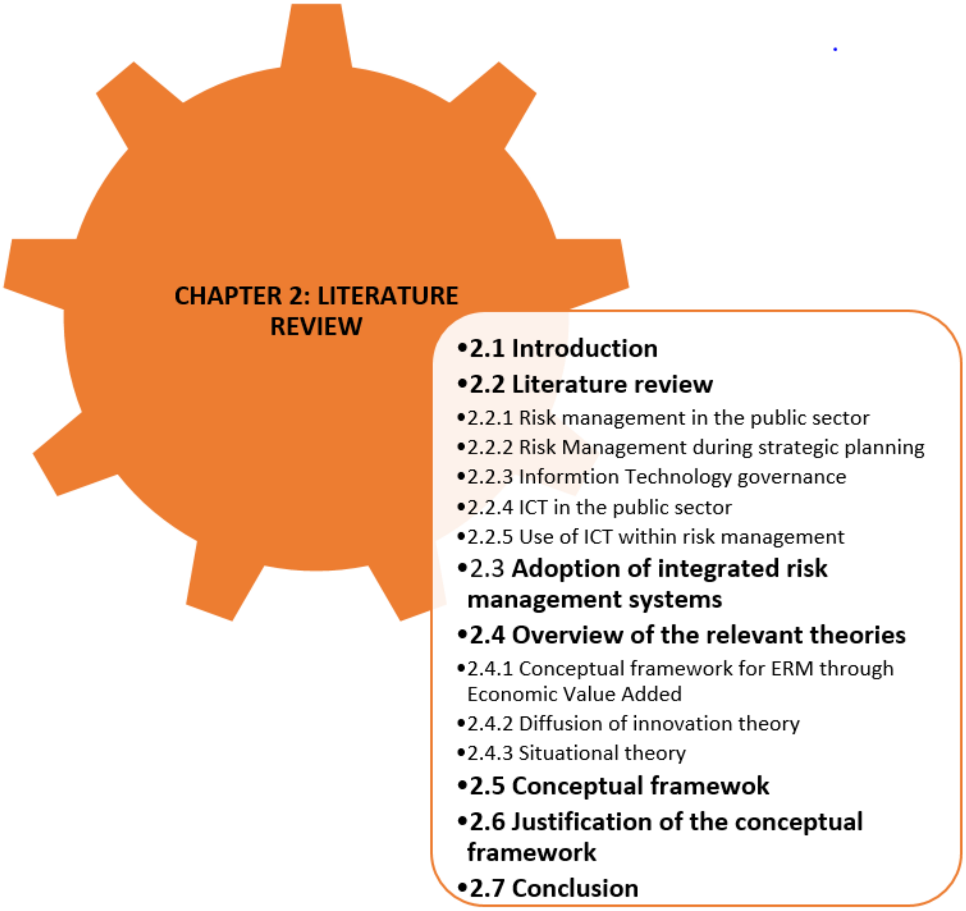

CHAPTER 2: LITERATURE REVIEW
•2.1 Introduction
•2.2 Literature review
•2.2.1 Risk management in the public sector
•2.2.2 Risk Management during strategic planning
•2.2.3 Informtion Technology governance
•2.2.4 ICT in the public sector
•2.2.5 Use of ICT within risk management
•2.3 Adoption of integrated risk management systems
•2.4 Overview of the relevant theories
•2.4.1 Conceptual framework for ERM through Economic Value Added
•2.4.2 Diffusion of innovation theory
•2.4.3 Situational theory
•2.5 Conceptual framewok
•2.6 Justification of the conceptual framework
•2.7 Conclusion

Figure 2.1: Chapter 2 layout

2.1 INTRODUCTION

This chapter reviews the existing literature on the implementation of risk management within the public sector through all literature reviews. The reviewed literature contributes to the proposal of the model to integrate ICT in the public sector. The chapter further provides the theories that underpin this study with the justification of the selected framework. The theories relevant to this study include a conceptual framework for enterprise risk management through Economic Value Added (EVA), diffusion of innovation theory, and situational theories. This chapter demonstrates the relationship between the selected theories within this study. To give context and justify the focus of this study, Section 2.2 of this chapter provides a literature review.

2.2 LITERATURE REVIEW

According to Nakano and Muniz (2018), literature reviews provide a comprehensive view that underpins the argument of the investigated subject. The researcher followed this approach to establish the theories about the use of ICT in risk management, determine the key concepts to shape the study and identify the gaps in the existing knowledge (Nakano & Muniz, 2018).

The literature review focuses on a plethora of studies relating to the use of technology in risk management. This review draws knowledge from the recommendations and conclusions from existing literature to guide this study. The reviewed literature provides a better understanding of the issues around ICT integration into risk management and provides a theoretical platform for the development of the model. The background of this study covers an extensive range of topics discussed in Sections 2.2.1 to 2.2.6.

2.2.1 Risk management in the Public Sector

The need for risk management (as defined in Chapter 1 as a process of identifying, analysing, and addressing risks) in the public sector is increasing owing to past financial and economic crises. This forced the organisations to confront the unforeseen risks brought by the COVID-19 pandemic (Yue et al., 2020). Based on risk management standards and principles, the risk management process is similar in both the public and private sector organisations. However, public sector risk management is seen to be more complex considering the responsibility and accountability thereof. While the private sector is accountable to its shareholders, the public sector is accountable to the public (Shand et al., 2022). Nel (2019) argues that rather than organisations viewing risk management as an alternative, the risk management process should be embedded into the organisation’s internal control systems to achieve their organisation’s strategic goals and objectives. This is critical for the organisation as this would entrench risk management in the culture of an organisation and therefore realise the benefits it promises. For this reason, Nel (2019) believes that organisations need to create risk awareness in their environment, especially in the public sector. Similarly, Zainudin et al., (2019) view risk awareness as one of the key elements in implementing risk management. While this is critical, Nel (2019) identifies leadership instability as a challenge in the public sector. The need to have sustainable risk management culture requires strong leadership that can set the tone from the top. While it is evident that the implementation of risk management is gaining prominence in the public sector, integrating risk management into managerial systems will improve risk management in the public sector (Bracci, Tallaki, Gobbo & Papi, 2021; Mahama, Elbashir, Sutton, 2020, Kong et al*.,* 2018). Integrating risk management in all the functions in the organisations will reduce the inefficiencies such as resource allocation, financial irregularities, and wasteful resources (Kong et al., 2018). As a result, incorporating risk management in corporate governance and strategic planning will ensure that all functional areas are involved in the overall decision-making of the organisation.

A strategic plan is a critical aspect that needs to be reviewed to determine how the risk management process is integrated into the planning process. The next section provides an overview of the strategic planning process in the public sector.

2.2.2 Risk Management During Strategic Planning

Kanu (2020) defines strategic planning as a systematic approach to defining a strategy to achieve its long-term goals and objectives. This process is important as the decision-makers can make informed decisions about where resources get allocated to support the achievement of these goals and objectives. Committee of Sponsoring Organisations (2017) and International Organisation for Standardisation (2018) encourage organisations to integrate enterprise risk management in their strategy setting. However, Kanu (2020, p3) indicates that organisations "still fail to adopt an integrated approach". The public sector organisations conduct the strategic risk assessment against their strategic objectives. Yet it is not clear whether this process is conducted concurrently with the strategic planning process (Nel, 2019). It is critical to note that risk management activities can be grouped into three categories, namely the organisational level, the mission and business process level, and the information system level (Iorga & Anil, 2016). All three levels are influenced by the decisions made by the strategic planning of an organisation.

Furthermore, to support the strategic risk assessment process, Nel (2019) suggests that public sector organisations should have a risk management committee, an audit committee, and an audit unit. It is important to have a risk management committee to provide an oversight function for the implementation of the risk management process in the organisation, including an authority to recommend the procurement of audit services to improve the organisation's reporting system (Larasati, Ratri, Nasih & Harymawan, 2019).

The next section provides an overview of the implementation of IT Governance to support the strategic objectives set during the strategic planning session.

2.2.3 Information Technology Governance

Usman (2019) avers that IT governance creates an environment for the organisation to align IT to its business strategies. This process allows an organisation to identify and manage IT risks aligned with the business strategy. The IT risks include the threats associated with the organisation's information technology assets and infrastructure (Mohammad, 2020). The National Institute of Standards and Technology (2018) warns that the organisation needs to understand the status of its assets such as servers, desktops, laptops, and network appliances for an informed decision-making process. Likewise, IT governance plays a key role in the sustainability of an organisation; it is important to observe the relationship between IT governance and the performance of the organisation (Ali et al., 2021). For this reason, organisations should prioritise innovation to maximise service delivery while not overlooking the risks triggered by these innovative technologies.

It becomes critical to determine whether the IT tools are effectively managed to support business processes. The public service sector in South Africa adopted the Corporate Governance of ICT (CGICT) which is informed by the Control Objectives for Information and Related Technologies (COBIT) framework that contains the process of managing risk - APO 12 (Department of Public Service Administration, 2012). The COBIT 5 framework was updated to the COBIT 2019 in 2018 (Information Systems Audit and Control Association, 2019). This framework (adopted by the cabinet in 2012) pays attention to the accountability and responsibility of the information technology activities within the departments. The CGICT needs to be implemented in the departments and facilitated by various stakeholders, with the IT officer leading the process as well as the risk management and audit teams also participating in the process (Department of Public Service Administration, 2012). The processes involved in the CGICT include the evaluation and direction of how ICT is used and monitored to ensure the achievement of the organisation's objectives. To support the departments in implementing this framework, a governance and management framework was developed to address, among other things, the management of IT-related risks (Department of Public Service Administration, 2012). Various departments institutionalised this framework by aligning it to their mandate (Department of Co-operative Governance and Traditional Affairs, 2018). The departments were required to develop their own strategies to implement the CGICT, which resulted in the development of the ICT management plan as their strategy.

The use and management of ICT in the public sector need to be explored to determine the appropriate approach to utilise ICT to improve the risk management process. This is discussed in the following section.

2.2.4 ICT in the Public Sector

ICT is closely connected to IT in various ways. Ratheeswari (2018) differentiates ICT from IT in that ICT is associated with the mechanisms that assist organisations to communicate information effectively and efficiently. This information is communicated through technology tools; hence IT is associated with managing information using computers and related technologies.

The role of ICT is to support the implementation of the organisation's developed strategies to ensure the accountability and achievement of these strategies (Qammaz & AlMaian, 2018; Kim & Kim, 2020). The COVID-19 pandemic forced the public sector to maximise the use of ICT beyond the office. It is during lockdown that the use of ICT became a fundamental resource to the work-from-home approach (Rachmawati et al., 2021). This is an indication that organisations critically depended on ICT as an enabler for the achievement of their objectives. Therefore, for the public sector to successfully implement ICT, the adoption of ICT becomes critical to understand the resources required and their capabilities (Gholami et al., 2021). While the adoption of ICT may need to be mandatory, it is important to acknowledge that there are different stages to ICT adoption as explained in Rogers' framework of diffusion of innovation (1995). Diffusion of innovation is a process where innovative interventions are communicated among individuals to improve existing processes (Mkhize, Mtsweni & Buthelezi, 2021).

The study conducted by Nazir and Khan (2022) reveals that there are factors that impact the adoption of ICT that may need to be addressed to achieve possible ease of adoption. These factors include cultural, internal and external, regulatory, and institutional support factors. Furthermore, Mkhize and Davids (2021) posit that a lack of IT infrastructure negatively affects ICT adoption, especially within the education sector.

In conclusion, there is a low IT adoption rate in the public sector which may be influenced by various challenges, including declining confidence in technological capabilities and the digital divide (Gholami et al., 2021). To address these challenges, an analysis of the strengths and weaknesses of the public sector in relation to ICT may be required (Uctu & Essop, 2020). While ICT is used in the public sector, it is critical to determine the impact of ICT on risk management effectiveness and whether it influences the overall performance of the organisation. The next section examines how ICT is used within risk management.

2.2.5 Use of ICT within Risk Management

It is evident from Section 2.2.4 that IT is justified to be a tool that supports business functions or processes for effectiveness and efficiency (Naidoo & Hoque, 2018). The outbreak of the COVID-19 pandemic forced public sector organisations to embrace technology for their business operations. Although some of the officials were able to operate remotely with the aid of technology, the organisations were confronted with bad risks that negatively affected business operations (Zhong et al., 2021). This suggests that having technology integrated into all risk management activities will enable the effective implementation of the risk management process.

There are limited research studies on the use of technology to support risk management in the public sector. However, numerous researchers value the impact of ICT on risk management. In exploring the aspects of risk management implementation for the Fourth Industrial Revolution (4IR) known as Industry 4.0. Simota et al., (2019) highlight that innovative approaches, improved frameworks, and complex IT infrastructure may pose new risks. Chanopas, Krairit, and Khang (2015) stressed that the IT infrastructure is a critical asset that an organisation needs to consider when introducing innovation. Industry 4.0 is viewed as a “strategic initiative” that exploits innovative technologies for efficient business operations (Brocal, González-Gaya, Komljenovic, Katina & Sebastian, 2019). In the same vein, this supports several researchers who highlighted the challenges resulting from the advanced technologies such as poor IT infrastructure and lack of resources among many things (Bvuma & Marnewick, 2020). The organisations, therefore, should advocate the capacitation of the users with new technologies and the risks it poses. While Industry 4.0 is aimed to bring efficiency through automation, it is not exempted from possible risks and challenges (Simota et al., 2019). Birkel et al., (2019) underscore the importance of identifying potential risks in line with the advancement of technology and managing them through the accepted risk assessment process. This means that, as organisations embrace the use of ICT in implementing risk management processes, they should be mindful of the potential risks around the use of ICT. In this way, sufficient resources can be allocated to effectively address these risks.

Marx and Schutte (2018) believe that organisations should integrate technology into their business processes. Weeserik and Spruit (2018) concur with Ali et al., (2021) on the integration of technology suggesting that it allows organisations to optimise their performance while maximising the benefits of technology. While the study conducted by Mishchenko, Naumenkova, Mishchenko, and Dorofeiev (2021) focused on financial institutions, this study encourages organisations to utilise a risk-based model to manage the risk related to technology integration. Furthermore, this study proposes that organisations should have a suitable organisational structure, appropriate risk assessment methods, and tools, as well as an information system to support the effective implementation of risk management. While a suitable organisational structure is important, an integrated risk management system is key for effective implementation of risk management.

The recent studies on integrating innovation in risk management suggest that artificial intelligent has the potential to have a positive impact on the effectiveness of risk management (Shabbir & Gardezi, 2020, Hussain, 2022; Drydakis, 2022 and Park & Singh, 2023). Hussain (2022) emphasised the importance of risk management being collaborative to realise the benefits of the available technologies such as data analytics to achieve its mandate. Furthermore, the adoption of artificial intelligent in risk management reveals the relationship between data analytics with the overall organisational performance improvement (Shabbir & Gardezi, 2020). Drydakis (2022) argues that while artificial intelligence positively impacts the capabilities of the organisation, this adoption of such technologies contributes to the effectiveness of risk management hence the improvement of the organisational performance. To fully benefit from these technologies, adequate IT infrastructure is critical to support the development of an effective risk management tool (Park & Singh, 2023). Based on the reviewed studies, the researcher observed the similarities between the literature and what this study intends to achieve. Overall, utilising innovative technologies in risk management has the potential to improve the effectiveness of risk management while bringing efficiency in implementing complex business operations such as projects (Akatov, Mingaleva & Klačková, 2019; Mishchenko et al., 2021).

The next section discusses the adoption of an integrated risk management system to support the proposal of the framework to integrate ICT into risk management.

2.3 ADOPTION OF INTEGRATED RISK MANAGEMENT SYSTEM

The public sector in South Africa has adopted the Enterprise Risk Management (ERM) approach to implement risk management (Department of National Treasury, 2010). The Public Sector Risk Management Framework (PSRMF) was developed in 2010 with supplementary documents being developed by the departments, such as the DWS risk management policy, framework, and strategy (Department of Water and Sanitation, 2021b). This framework was guided by the International Organisation for Standards 31000: 2018 (Alijoyo & Norimarna, 2021) and the Committee of Sponsoring Organisations of the Treadway Commission (Schandl & Foster, 2019; Martens & Rittenberg, 2020). In contrast to the ERM framework, Control Objectives for Information and Related Technologies (COBIT) framework was adopted for the effective governance and management of IT resources (Information Systems Audit and Control Association, 2019).

The PSRMF is aimed at implementing risk management in all critical areas of the organisation in a systematic approach (Department of National Treasury, 2010). This framework is being implemented to enforce the integrated risk management approach with the risk management teams having been the drivers while leadership played a key role in this process. With senior management owning the ERM process, it is ensured that risk management is embedded across the organisation. The ISO 31000: 2018 standards provide guidelines and principles to assist organisations to establish effective risk management processes (Alijoyo & Norimarna, 2021). Furthermore, the Institute of Risk Management (2018) asserts that the revised ISO 31000:2018 standards provide a more clear and simple guide to assist organisations in better planning and making more informed decisions.

The COSO framework developed in 2004 provided the organisation with the guidance to implement an enterprise-wide culture of risk management (Everson et al., 2017). In the latest COSO framework, Schandl and Foster (2019) introduced an aspect of integrating risk management strategy with the performance of an organisation. Furthermore, Foster (2019) postulates that this framework is a blueprint for creating a conducive internal control environment for an improved risk management process. In short, the COSO framework complements the PSRMF by assisting the organisation in linking the organisational strategy, risk, and the performance of the organisation (Committee of Sponsoring Oganisations, 2016).

The COBIT framework is an IT governance guide for the public sector to govern and manage its IT resources. Information Systems Audit and Control Association (2019) warns that this framework is not designed for the IT department but the entire organisation to ensure that information and technology are managed properly to achieve the goals of the organisation. While the COBIT framework guides decision-making of the top management of the organisation within the entire IT operations, ISO 27001 focuses on the security management of IT assets. The organisations are required to conduct IT security risk assessments on planned intervals which could be implemented annually and when new changes emerge (Kitsios, Chatzidimitriou & Kamariotou, 2022). The IT security risk refers to a threat affecting the use and operation of an information system such as hardware, software, and ICT networks (The Information Technology Authority - ITA, 2017). Likewise, the COBIT framework also resonates with the notion of an enterprise-wide risk management approach.

All these frameworks have one thing in common where the focus is on effective risk management implementation for the achievement of the organisation’s objectives. For the organisation to perform, IT resources should be effectively managed as they may have a positive impact on effective risk management (Schutte & Marx, 2018). Ettish (2017) argues that for organisations to realise “optimal IT governance”, risk management frameworks need to be integrated to avoid silo approaches. Ako-Nai and Singh (2019) point out the structural, process, and relational capabilities as the key capabilities structured that organisations require to achieve optimal IT governance. These capabilities synchronize with the theoretical concepts that are grounding this study. The concepts of structural and process are sufficiently defined in Section 2.4 while relational capabilities are not discussed. The relational capability allows all the strategic stakeholders to jointly make IT-related decisions through engagements and collaboration (Ako-Nai & Singh, 2019; Salisu & Bakar, 2020). This echoes the sentiments on the importance of integrating risk management activities, hence integrating all the risk management frameworks is crucial (Weeserik & Spruit, 2018; Kanu, 2020). In support of this argument, Marks (2019) underscores the need for organisations to consider a variety of different approaches as one framework may not be a perfect fit for the organisation. Algheriani, Kirin, Vidosav, and Spasojević-Brkić (2019) raise the possibility of the conflict of operations and inefficiencies of management when multiple standards are implemented. However, the National Institute of Standards and Technology (2020) states that these frameworks generally adopt a similar approach to the risk assessment process. The compatibility of these frameworks with each other brings the potential to develop an integrated model that is comprehensive for the organisation (Algheriani et al., 2019).

To provide the structure for this study, the theories relevant to the use of ICT in risk management are reviewed. The theories encompass concepts and premises that are connected and relevant to this study, while a conceptual framework justifies the study considering known knowledge (Varpio, Paradis, Uijtdehaage & Young, 2020).

The next sections provide insights into the overview of the theoretical theories (Section 2.4), the conceptual framework developed from the existing theories (Section 2.5), the justification of the conceptual framework, and how the study is viewed through the lens of the selected concepts (Section 2.6).

2.4 OVERVIEW OF THE RELEVANT THEORIES

A theoretical review highlights the existing theories such as the Conceptual Framework for Enterprise Risk Management (ERM) through Economic Value Added (EVA), diffusion theory, and situational theory that underpins this study. These theories are discussed in Sections 2.4.1 to 2.4.3.

2.4.1 Conceptual Framework for ERM through EVA

According to Varpio et al., (2020, p1), researchers are expected to “articulate the use of theory, theoretical framework and conceptual framework” in their studies. Researchers must understand the distinction and relationships between these concepts and how they shape their studies (Varpio et al., 2020). Varpio et al*.,* (2020) define theory as an abstract that explains some concepts that make researchers understand the world through, among other things, describing, explaining, and predicting the phenomenon. Theoretical framework uses theory or theories to articulate how the research will utilise new knowledge (Nhan, 2020). Adom, Hussein, and Agyem (2018) argue that both the theoretical and conceptual frameworks provide the path and theoretical grounding for the research and play a key role in making the research findings more meaningful. Yet, while both frameworks provide grounding for the study, the two frameworks differ. The theoretical framework draws from the existing theoretical literature relevant to the study while the conceptual framework incorporates all aspects of the research (Mensah, Frimpong & Acquah, 2020).

Adom et al., (2018) underscore the importance of selecting an appropriate theory or theories that affirm the knowledge of the investigated phenomenon. Three theories underpinned this study: the conceptual framework for enterprise risk management through Economic Value Added (EVA), the diffusion of innovation, and the situational theory. The selected theories were chosen as they resonate with the definition of the research problem in this study, the literature review, and the methodology. The grounding of the concepts in these theories explains the use of ICT in risk management and the extent to which it is used, as well as the behaviour of the users in respect of adopting ICT. Furthermore, the concepts in the three theories resonate with the national integrated ICT policy White Paper that was approved in 2006.

The theory on the conceptual framework for ERM through EVA, as illustrated in Figure 2.2, is a framework that assesses how ERM positively influences the performance of the organisation using EVA.

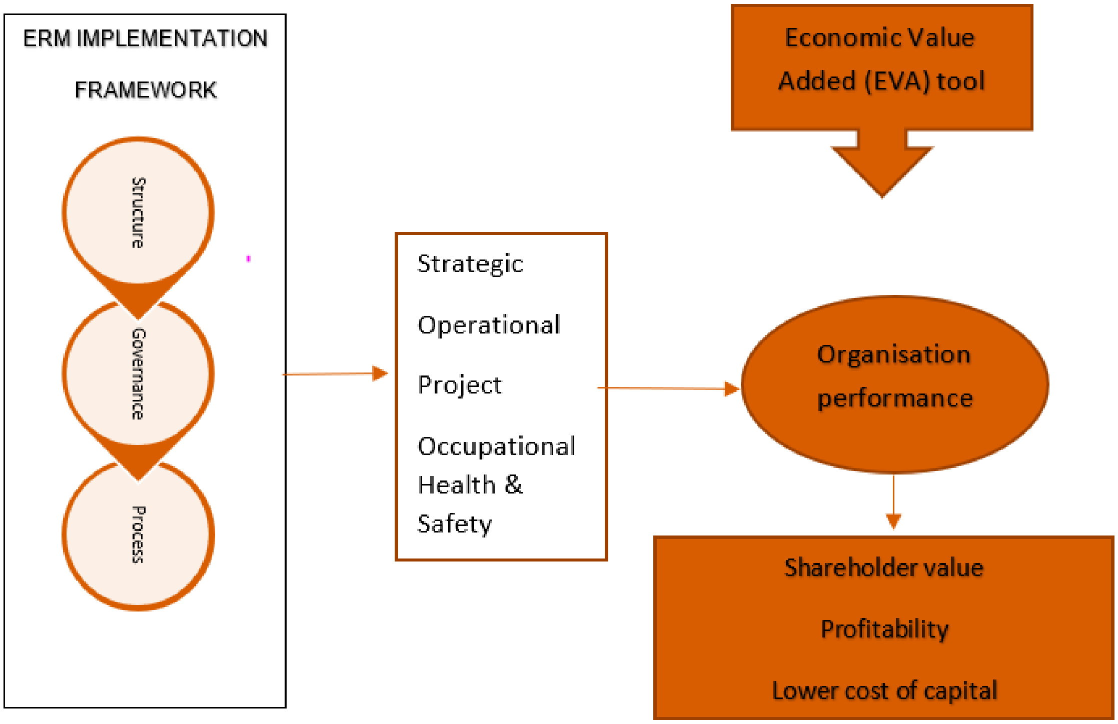


Figure 2.2: ERM through EVA

EVA is a tool that is used to measure the performance of an organisation by comparing the remaining profit against the total cost of capital (Noronha & Pamnani, 2021). There are limited studies conducted in the public sector that unpacks the conceptual framework for ERM through EVA. As this study is within the public sector, the performance of an organisation is measured through service delivery. While this study does not determine the impact of using ICT to improve performance but the effectiveness of risk management, the researcher believes that the overall aim of implementing risk management is to improve the performance of the organisation. This made this theory to be relevant.

Martens and Rittenberg (2020) underscore the significance of ERM in managing the organisation's risk; hence the effectiveness of the risk management process is key. For risk management to be value-adding and to impact the performance of the organisation, the risk management process needs to be effective (Schutte & Marx, 2018; Marks, 2019; Alijoyo & Norimarna, 2021). Annamalah, Raman, Marthandan, and Logeswaran (2018) state that this framework is based on an ERM model that comprises structure, governance, and process. Kong et al., (2018) define these aspects as follows:

- The structure is concerned with providing the organisation with an enabler or architecture to understand the risk areas and to communicate them effectively. The ERM structure ensures, among other aspects, that a technological environment is created to support the implementation of risk management.
- The second aspect is the ERM process which ensures that all risk management activities are integrated into all business strategies for the achievement of the organisation's objectives.
- Lastly, ERM governance creates structures to allow for the identification and management of business risks in a structured approach. The organisation needs to ensure that all three aspects are in place for the appropriate implementation of ERM if they are to achieve its objectives.

Zainudin et al., (2019) argue that the assessment of the organisation's performance can be influenced by the informed decisions it takes and how the organisation allocates resources. All of this is influenced by the assessment and monitoring of the organisation's risks. Likewise, Akatov et al., (2019) view effective ICT as an essential element of the organisation's efficiency and effectiveness. It is concluded that the conceptual framework for ERM through EVA is useful for this study as it has proven that with the three aspects in place, risk management promises a potential achievement of the objectives and improved organisation performance. Section 2.4.2 discusses the second theory, the diffusion of innovation theory, to understand how users embrace innovation.

2.4.2 Diffusion of innovation theory

Dearing and Cox (2018) define diffusion of innovation theory as a social process of how people respond to learning and embracing innovation. This study intends to determine the impact of using innovation to improve risk management processes. Countless ICT tools may be used to manage risks and communicate risk-related information among the officials and the risk management governance structures, however, it is important to understand how people in the organisation embrace technology tools. Dearing and Cox (2018) argue that, in some cases, effective innovative mechanisms fail to be diffused regardless of their effectiveness. It is crucial to determine the reasons for these failures to gain insight into the social environment. This will assist organisations in better planning, as they are aware of the nature of their environment, and what drives the willingness to embrace innovation. Shava and Vyas-Doorgapersad (2021) accentuate that the theory of diffusion of innovation was perceived as valuable in understanding the utilisation of ICTs in government organisations. To determine the impact of using ICT in the DWS, this makes diffusion of innovation theory to be relevant for this study.

While the risk management team may be willing to embrace technology, factors beyond their control might delay the technology adoption. The next section discusses the situational theory to understand the factor that contributes to the use of technology in risk management.

2.4.3 Situational theory

The purpose of the situational theory developed by Hersey in 1984 is to determine the internal and external factors that impact the success of an organisation which includes identifying the problem, level of involvement, and constraint recognition (Hakim, Faizah & Mas'adah, 2021). This theory is useful for this study as it will assist in understanding the factors affecting the use of ICT, or lack thereof, in risk management. Thompson and Glasø (2018) highlight competence and commitment as the critical elements of situational theory. Thompson and Glasø (2018) further define these concepts starting with competence as the knowledge, and skills gained through formal education, as well as experience gained on-the-job training. For this study, competence is critical as the participants need to be conversant with risk management practices and technological advancement in the public sector. The second concept of commitment investigates how motivated and confident the individuals are. This is also key for this study as it may be possible that the users are provided with ICT resources but owing to the lack of motivation and confidence, they do not utilise these resources.

While the above theories were deemed relevant for this study, only specific concepts from these theories were joined to form the conceptual framework to guide the development of the model to integrate ICT into the risk management process. Section 2.5 discusses the conceptual framework.

2.5 CONCEPTUAL FRAMEWORK

A conceptual framework can be viewed as a graphic illustration of how theoretical concepts that grounds the study relates to one another in shaping the research (Mensah et al., 2020). Figure 2.3 illustrates the conceptual framework developed from the selected theories with a focus on the key concepts combined with the existing theories discussed in Section 2.4.

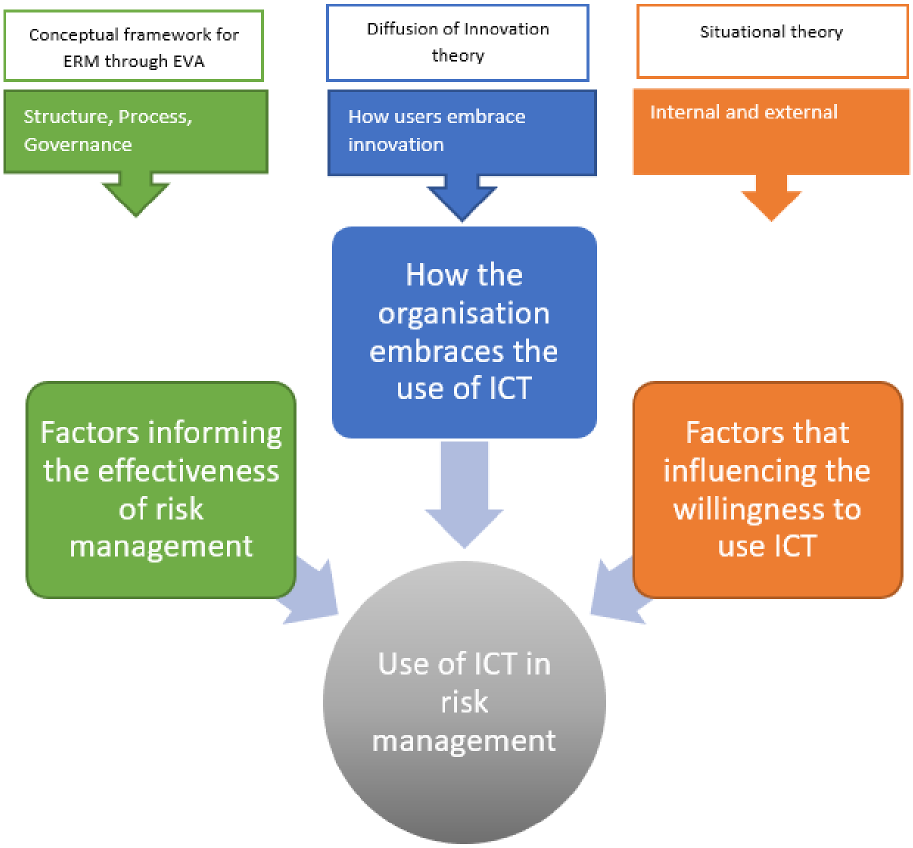

Conceptual framework for ERM through EVA
Diffusion of Innovation theory
Situational theory
Structure, Process, Governance
How users embrace innovation
Internal and external
How the organisation embraces the use of ICT
Factors informing the effectiveness of risk management
Factors that influencing the willingness to use ICT
Use of ICT in risk management

Figure 2.3: Conceptual framework

The conceptual framework postulates that technology through ICT tools contributes to the effectiveness of risk management. As depicted in Figure 2.3, these factors are structure, process, and governance. Larasati et al., *(*2019) view the effective implementation of ERM as the state where there is a structure that enables the communication of risk factors throughout the organisation. Interestingly, a study on the role of IT in risk management highlighted that, for ERM programmes to be effective, governance structures and processes should integrate risk-based decisions (Schutte & Marx, 2018). These three concepts guide the determination of the organisation's risk management context. The ISO 31000 (Alijoyo & Norimarna, 2021) posits that the risk management process needs to support the development and implementation of the organisation's strategy. For this study, the risk practitioners, risk champions, and risk owners operate within the public sector risk management framework. This framework refers to an enabling environment that creates a risk management culture in an organisation. It further refers to the structures to support the implementation of the risk management processes.

These processes are integrated with the governance structures to play an oversight function over the risk management performance. Risk practitioners are the key drivers of risk management in the organisation. Their responsibility includes establishing a risk management structure in the organisation. Owing to the size of the organisation, the risk champions play a critical role in supporting both the risk practitioners and the risk owners. The risk owners are the key custodians of the risk management process in their respective areas of responsibility. The three parties ensure the implementation of the public sector framework in the organisation. To determine the impact of ICT on the effectiveness of the risk management process defined in this section, it is critical to investigate how the organisation embraces innovation.

The organisation's attitude towards embracing innovation is influenced by numerous factors (internal and external) that contribute to the willingness of the organisation to adopt ICT. This is informed by how the users utilise ICT through the available technologies within risk management to enhance the risk management process. One of the contributing factors to addressing service delivery challenges in the public sector is innovation. Admittedly, the public sector is viewed as ineffective when it comes to innovative management strategies (Shipalana, 2020). Some other factors contributing to ineffective innovative strategies, as alluded to by Shipalana (2020), are poor communication and coordination. These factors are critical as adopting innovation is informed by the level of engagement with the stakeholders and skills related to technology. These factors have been highlighted in the literature reviewed in this study. For this study, the diffusion of innovations theory by Rogers (1962) assists in determining how users respond to learning and embracing the use of ICT in the organisation and advancing the adoption of ICT. It is worth noting that users adopt innovation only once they have accepted it (Kim & Kim, 2020). Considering the role of the risk practitioners, champions, and owners, the five categories of adopters (Rogers, 1995) will be used to examine the participant's behaviour toward using ICT in risk management, as illustrated in Figure 2.4.

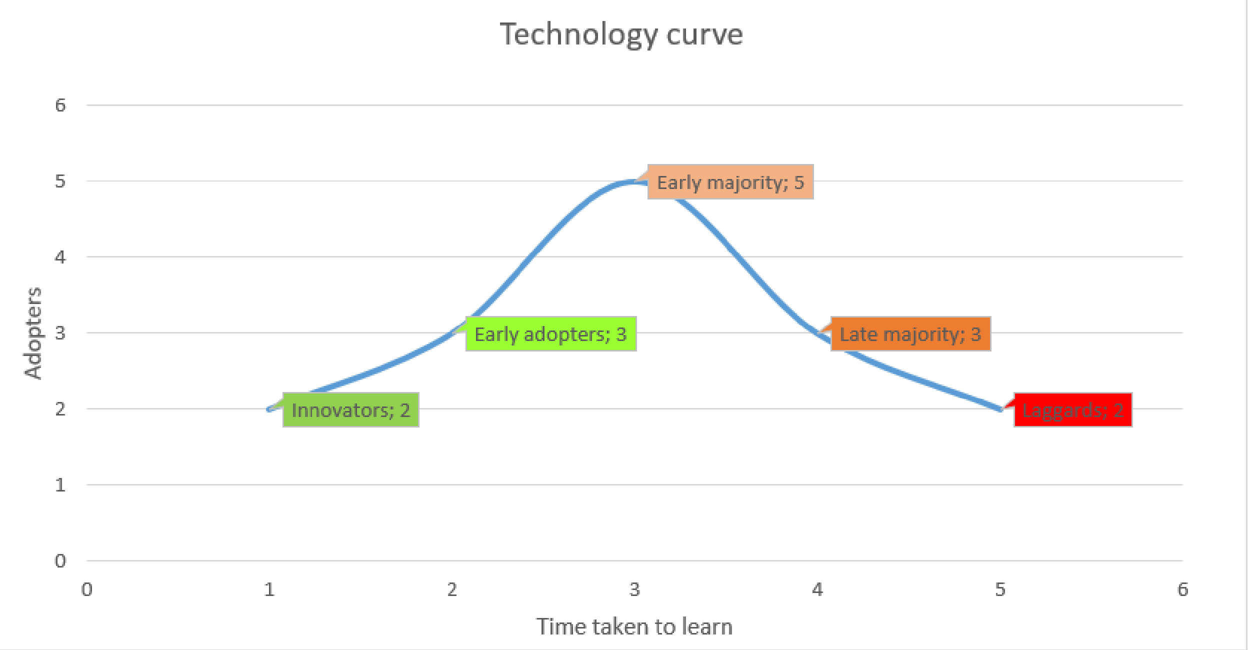


Figure 2.4: Technology adoption curve

Source: Dearing and Cox (2018)

Figure 2.4 illustrates the time taken by the adopters to learn and adopt ICT. As depicted in Figure 2.4, only a few adopters decide to adopt innovation, and these are referred to as innovators as they are eager to try innovative ideas. The next after the innovators are the early adopters who decide to adopt based on the influence of their leaders. The early majority follows suit deliberately followed by the adopters who follow once the majority have attempted innovative technology. The last group to follow is the laggards – this group waits for technology to become part of the tradition before adopting it. The COVID-19 pandemic has forced a shift to the public sector organisation where different approaches have been exhausted. The report produced by KPMG on modernising the public sector revealed that the public sector is adopting technology at a faster pace during the pandemic period (Forsyth, 2021). It is important to examine where the technology users fit in these five adopters' categories to support this shift.

Lastly, unpacking the factors affecting the willingness of the users to utilise ICT, particularly in risk management, changes the perspective of the organisation embracing innovation. This provides an opportunity to address these factors, giving rise to a change in how the users view technological changes. The two dimensions taken from Hersey and Blanchard's situational theory (Thompson & Glasø, 2019; Shaikh & Shaikh, 2019) are leadership and behaviour. The leadership of the organisation should have the ability to support and direct the employees (who are the users of technology in the case of this study) towards a change of behaviour that gradually changes their willingness to adopt ICT (Thompson & Glasø, 2019). The gradual change of the behaviour will lead to the development of the users which allows for the assessment of the behaviour toward the use of ICT and the efficiency of risk management thereafter in the context of this study.

2.6 JUSTIFICATION OF THE CONCEPTUAL FRAMEWORK

To establish the approach for this study, it is critical to find concepts from the existing theories that can provide the study with a structure and vision. These concepts provide lenses through which the research problem could be viewed and shape the analysis of data relevant to the study. The key aspects of this study are to understand the extent to which the ICT resources are made available, accessed, and utilised, the contributing factors to utilising ICT resources to support the risk management process, and later to understand whether IT risk assessments are conducted in the public sector.

Understanding how ERM positively influences the performance of the organisation is the starting point towards the realisation of whether the risk management process in the organisation meets the criteria of being effective. The assumption is that, for risk management to influence organisational performance, it needs to be effective. The conceptual framework for ERM through EVA provides three important aspects that allow risk management to add value. These are the structure, process, and governance. These three aspects allowed the researcher to take the phenomenon further by making another assumption that ICT contributes to the effectiveness of risk management. Without the foundation of risk management (structure, process, and governance), it is impossible to link the use of ICT to the effectiveness of an "unknown" risk management process. Understanding the availability and access to ICT resources in risk management will allow the researcher to investigate whether these resources are utilised or not. The concept of embracing innovations will provide the grounding to understand whether the users are willing to utilise the resources made available to them. Lastly, the determination of whether these resources are utilised or not will require the researcher to examine the contributing factors to the use or lack of ICT resources in risk management. It was on these grounds that these concepts were deemed appropriate for this study.

The literature review reveals that risk management needs to be embedded in the culture of the organisation; this can be achieved through awareness creation. With a risk-alert culture, organisations improve in implementing risk management. The key element to supporting the implementation of risk management is the use of technology-based tools. The public sector departments integrate risk management and ICT during the strategic planning session for the improved achievement of the targets. This process encourages the integration of ICT in all business operations, as the planning is done for the organisation rather than individual business units. Yet the limitation of resources and skills may be detrimental. The identification and management of these limitations and challenges need to be addressed. Generally, ICT is used as an enabler in the public sector although technological change potentially triggers new risks that have negative implications on the use of ICT.

2.7 CONCLUSION

Having argued on how ICT affects the implementation of risk management processes, a conclusion was drawn based on the literature reviewed. Organisations in the public sector need to invest in ICT when considering the impact ICT may have on supporting risk management implementation. Several ICT shortcomings have been identified with the recommendation that they need to be addressed. These shortcomings included limited access to ICT, inadequate or lack of ICT knowledge and skills, limited financial resources, and inadequate internal control environment, among other things. It was also critical that, while organisations were appreciating the role played by ICT, organisations need to ensure that ICT is fully integrated within the business processes. It was concluded that simply just utilising ICT is not sufficient as how it is used is vital. The organisations need to develop ICT strategies to support risk management. The developed strategies need to be implemented and tested to confirm their viability.

The consulted literature for this study motivated the need to determine the effects of using ICT to support risk management within the public sector. In line with sub-objective 1, to a certain extent, ICT was used to implement risk management processes in the public sector, yet literature suggests that there is still an opportunity for improvement. To answer sub-objective 2, it was not clear whether ICT is integrated into all risk management activities, but there were some areas where there was evidence that ICT was integrated. Lastly, to answer sub-objective 3, it was also clear that some public sector departments conduct the IT risk assessment mostly on a strategic level, yet it was not clear whether IT risk assessments are conducted for the IT resources that support the implementation of risk management. Beyond determining the ICT contribution to risk management, the framework that this study proposes, considers the key issues raised from the literature review, including the integration of various frameworks as indicated in Section 2.3. To gain an in-depth view of these objectives, data were collected and analysed to determine the extent to which these objectives were achieved. The next chapter provides the research methodology for the study.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter provides an outline of the procedures and methods that this study followed to collect and analyse data. The layout of this chapter is diagrammatically presented in Figure 3.1. This chapter is structured as follows: Section 3.1 provides the introduction, Section 3.2 discusses the research design, and measuring trustworthiness in the study through credibility and objectivity is discussed in Section 3.3, while Section 3.4 addresses ethical considerations. The conclusion is provided in Section 3.5.

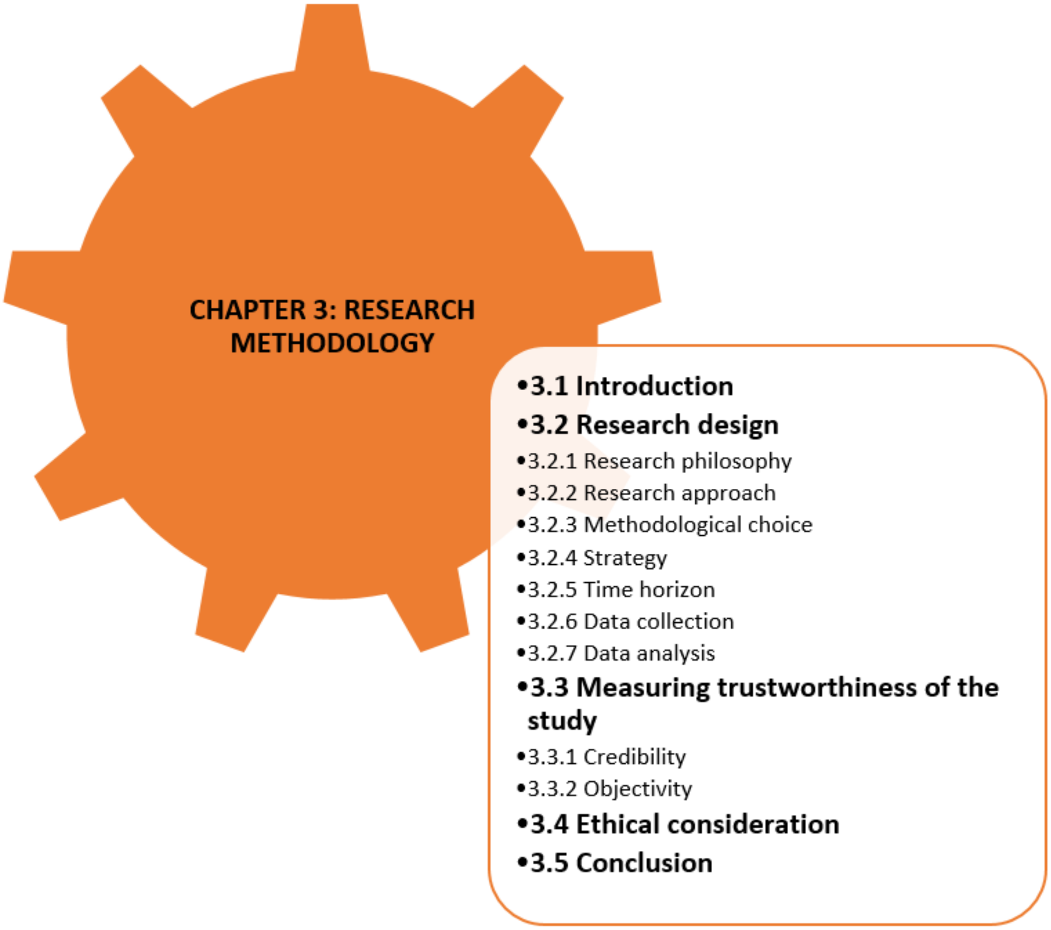


Figure 3.1: Chapter 3 layout

3.1 INTRODUCTION

The previous chapter presented the literature review including the theories that underpin this study. This chapter outlines the research design and methodology followed to achieve the research objective of the study, which was to determine whether the use of ICT to implement risk management has an impact on the effectiveness of risk management. This research objective was achieved through the adoption of the research onion model (Saunders, et al., 2019), where each layer will be discussed to uncover the research process to be followed. Patel and Patel (2019) define research methodology as a systematic approach that the researcher adopts to conduct the research to address the research problem. Fernandez (2020) argues that the selection of a methodology depends on the perspectives that underpin the study. Goundar (2012) underscores the importance of understanding the type of research, strategy, philosophy, time horizon, approaches, and the right procedures and techniques for the study.

This chapter focuses on the research design and approach adopted following the research onion, elaborating on the design, population, sampling, and data collection methods. It further presents how the collected data were analysed to produce valid and tangible results.

3.2 RESEARCH DESIGN

Oshagbemi (2017) and Fernandez (2020) assert that the research design is an organised strategy that outlines data collection, measuring, and analysing data within the research. It is critical to note that the research design links the research question to the objectives of the study (Oshagbemi, 2017). A suitable research design is aligned with the research questions that the study intends to answer. Furthermore, Downs (1990) emphasises that the research problem needs to be clearly defined to have a good research design. For the achievement of the research objectives, this section details the sources of data collection and the choice of design informed by the research questions. The design that this study follows is the research onion layers proposed by Saunders, Lewis, and Thornhill (2019), as illustrated in Figure 3.2.

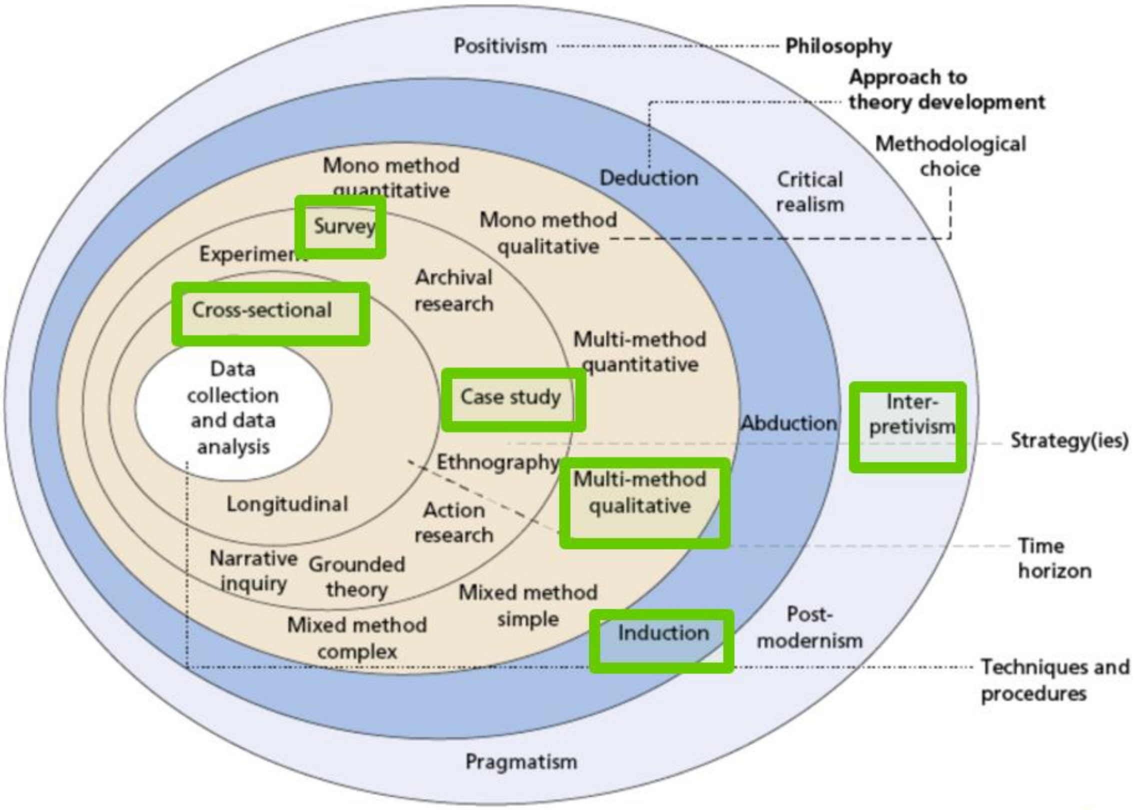


Figure 3.2: The Research Onion

Source: Saunders, Lewis, and Thornhill (2019)

The research onion was developed to specify the key phases that a researcher needs to follow to ensure a proper research process. The first two layers (philosophy and approach) of the research onion can be viewed as a process towards theory development (Saunders, et al., 2019). The third, fourth, and fifth layers consist of methodological choice (qualitative or quantitative), strategy (ethnography, case study, ethnography), and time horizon (longitudinal or cross-sectional). These three layers inform the process of the research design. Lastly, the sixth layer is the data collection and analysis.

This section commences with an overview of the research philosophy discussed in Section 3.2.1.

3.2.1 Research philosophy

Research philosophy is the first layer to be peeled as a basis of research. According to Saunders et al., (2019) and Mauthner (2020), research philosophy is a system in which knowledge is developed about the phenomenon that is being investigated. In developing knowledge, the researcher seeks to understand the beliefs that the participants have about the phenomenon. Three dominant paradigms are mostly used in research, namely the positivist, interpretivist, and critical realism paradigms (Kivunja & Kuyini, 2017), to organise data about the phenomenon. Table 3.1 provides an overview of these three philosophies.

Table 3.1: Research paradigms

(Source: Oates (2006))

POSITIVIST	INTERPRETIVIST	CRITICAL REALISM
Reality is real and understandable	Multiple local and constructed realities	Reality is real but only imperfectly and probabilistically understandable
Findings are true (objective)	Findings are created, and they are developed based on the interaction with the participants (subjective)	Findings are true (modified objectivity)
Deductive: general to specific. Concerned with testing theory and verification of hypotheses	Inductive: observation to theory. The researcher is passionate and a participant in the research	Can be both deductive and inductive. Interpretation is qualitative but also qualitative methods
Quantitative	Qualitative	Quantitative or qualitative

The positivism paradigm focuses on the scientific study of the social world where reality is not influenced by opinions and beliefs but rather by objectivity (Park, Konge & Artino, 2020). On the contrary, critical realism views reality as multi-layered and the findings are true as it is with the positivism (Lawani, 2020). These two paradigms were not relevant to this study, considering that the study had intended to create findings based on the views of the participants that may be subjective.

The researcher opted for the interpretivism philosophy, as indicated in the grey-shaded column in Table 3.1. According to Saunders et al., (2019), interpretivism allows the researcher to engage with the phenomenon to get an understanding of the subject and the interpretation based on the viewpoint of the participants. To elaborate more on interpretivism, Ryan (2018) argues that the research emphasises how the subject thinks and makes out the world surrounding them. Furthermore, Blumer (1986) maintains that the individual's viewpoints are influenced by the person's perception of situations and their social interactions, resulting in meanings being generated. Interpretivism was deemed suitable for this study as the researcher commenced the study with an insight into the contribution that ICT has on the business process. However, the researcher believed that there was more to uncover, specifically linking ICT to risk management in the public sector.

The next layer that needs to be peeled after the research philosophy is the approach layer, which will be discussed in the next section.

3.2.2 Research approach

The research approach is a plan that guides the researcher on the approach to take when gathering data for theory development. This layer provides an option to choose between the deductive and inductive approaches, as illustrated in Figure 3.3.

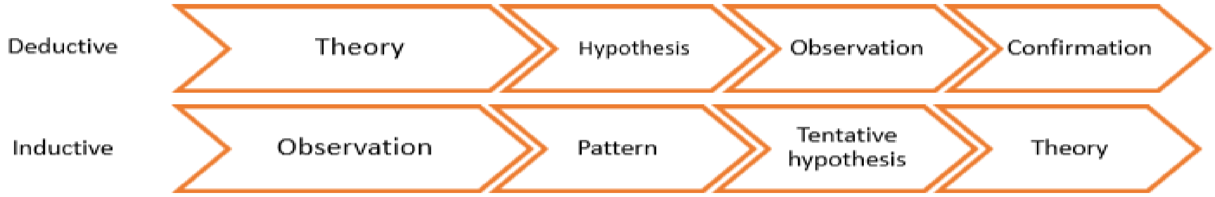


Figure 3.3: Deductive vs inductive

Source: Mitchell (2018)

3.2.2.1 Deductive

As defined by Saunders et al., (2019), the deductive approach is when the researcher begins with the existing theory and moves towards the hypotheses in carrying out the research process. This will either confirm or reject the premises of the study. Similarly, Patel and Patel (2019) concur that the deductive approach is where the researcher draws a conclusion from the existing theory and develops a strategy to test the hypothesis, while the inductive researcher starts with observations to find patterns from data and then develops a theory based on the observations. Fernandez (2020) argues that deductive research was valuable for the improvement of science. Owing to the nature of this approach, Mitchell (2018) views this approach as a top-down approach, for it commences with a more general view toward the specific. The deductive approach is concerned with testing an existing theory. Creswell (2009) indicates that when conducting deductive research in a quantitative study, a researcher starts with an existing theory (this theory is an outcome of the inductive approach). This means that without an existing theory, it is not possible to conduct this study as the hypothesis is formulated based on the existing theory.

3.2.2.2 Inductive

The inductive approach is concerned with creating new theories (Saunders, 2014). However, Bryman and Bell (2015) argue that the outcomes of the data analysis may be like that of the existing theory. It is for this reason that this approach is sometimes referred to as a bottom-up approach (Mitchell, 2018). Creswell and Creswell (2018) assert that, in analysing data, qualitative researchers build patterns and themes from the collected data until a comprehensive set of themes is established. Once these themes are clearly understood, the theory can then be developed. This study adopts an inductive approach for its potential to reduce the researcher bias during the data collection stage where there is no existing theory as it is informed by interpreting the participants' feelings based on the patterns from observations. More importantly, the researcher interacts with the participants through interviews and surveys to get their views on the subject. The researcher observes the patterns during these interactions and explores them to create a theory from the observations.

3.2.2.3 Abduction

In addition to deduction and inductive, another approach is called abduction. Rashid, Rashid, Warraich, Sabir, and Waseem (2019) define abduction as an approach that identifies and addresses any weaknesses for both inductive and deductive approaches. This approach observes reality and experience and then predicts the conclusion. It is critical to note that there is no certainty with this best prediction as an assumption is that there is a possibility that there is evidence that exists but was never presented. For this study, an assumption can be made that the risk management process is failing in the organisation based on the allegation that ICT is not being used. Furthermore, the concern for abduction is that it takes too long for data to be collected. Abduction is therefore not appropriate for this study as it will not give the full view of all the attributes that have an impact on whether risk management is effective or not.

The next layer that needs to be peeled after the approach is the methodology choice layer which will be discussed in the next section.

3.2.3 Methodological choice

After determining the approach adopted in this study, the next layer to be peeled is the methodology choice. The research question for the study informs the methodology choice. Moreover, methodology choice allows the researcher to decide on the kind of data that should be collected and how that data should be analysed, while offering various research methods that a researcher could choose from (Mardiana & Bandung, 2020). The research method is defined as the system of collecting, analysing, and interpreting data (Creswell, 2018). This layer presents the researcher with three methods of collecting data to choose from, namely mono, multi, and mixed qualitative or quantitative methods, as illustrated in Figure 3.4.

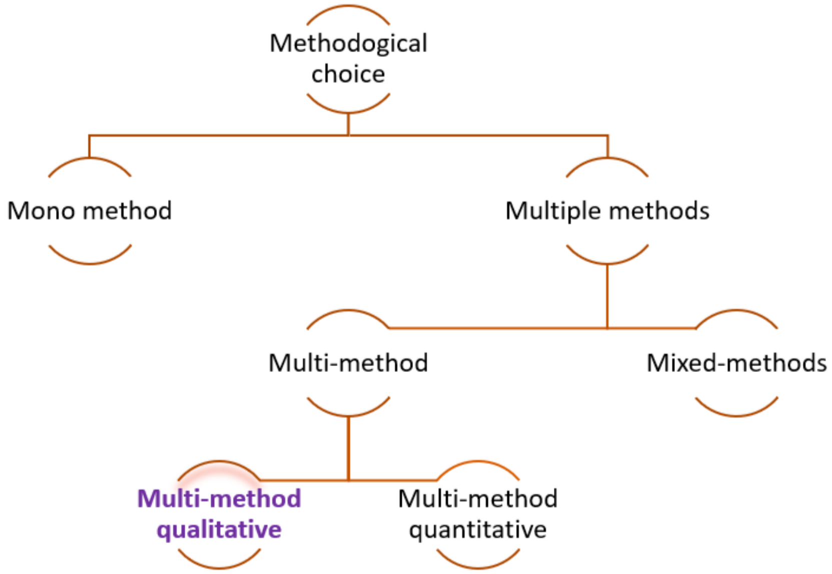


Figure 3.4: Method of collecting data

Source: Saunders et al., (2009)

Figure 3.4 illustrates the methodological choice where the researcher could apply either of the three methods, such as the mono, mixed and multiple methods. Saunders, Lewis, and Thornhill (2019a) make a distinction among these methods as follows:

3.2.3.1 Mono method

The Mono method is used when collecting single data using one method. In this case, a qualitative technique can be utilised with a qualitative data analysis procedure. This method was not suitable for this study as the study adopted two methods to collect data. Alternatively, the researcher can mix two methods. Section 3.2.3.2 discusses mixed methods.

3.2.3.2 Mixed methods

The researcher has the option to opt for mixed methods using both qualitative and quantitative data collection techniques and data analysis procedures. This method was not suitable for this study as the researcher adopted qualitative research, which requires qualitative data collection methods and qualitative analysis only. However, the researcher had the last alternative where multiple methods could be adopted. Section 3.2.3.3 discusses the multiple methods.

3.2.3.3 Multiple methods

The multi-method allows a researcher to use more than one data collection technique like interviews and questionnaires with a relevant data analysis technique (Anguera et al., 2018). A researcher may use either qualitative or quantitative data collection techniques and analysis. For this study, a multi-method qualitative approach was appropriate. The reason for choosing the multi-method qualitative approach was that it allowed the researcher to gain a full understanding of the subject at hand through triangulation. Triangulation is a method of data collection using a variety of methods to ensure a better understanding of a phenomenon and to cross-check the collected data (Noble & Heale, 2019; Nha, 2021). Triangulation aims to validate the results of the research study. The researcher can collect data for the same phenomenon from different stakeholders using different data collection methods. In this case, data were collected from various categories of participants, such as the risk champions, risk practitioners, and risk owners. The benefits presented by triangulation include enhancing validity by bringing in more than one method to substantiate the outcomes of the research (Ngulube, 2020). Furthermore, triangulation allows for the generalisation of the research to various research settings such as a broader group of organisations in the public sector (Bans-Akutey & Tiimub, 2021). According to Noble and Heale (2019), a researcher can select one of the four traditional types of triangulations in their studies:

3.2.3.3.1 Data Triangulation

Rugg (n.d.) defines data triangulation as a process where the researcher collects data from numerous data sources for the same study. Bans-Akutey and Tiimub (2021) argue that data triangulation allows the researcher to verify the results from more than one source, such as the participants and the stakeholders. This option was relevant for this study considering that data were collected from different groups of participants.

3.2.3.3.2 Investigator triangulation

According to Rugg (n.d.), investigator triangulation is a process of collecting data using multiple researchers for a specific phenomenon. The promotion of using various researchers using the same method allows for the verification of the findings. This option could be relevant for this study, yet it was impractical to get more researchers due to the time limitations of the study.

3.2.3.3.3 Theory triangulation

Theory triangulation is the process of collecting data using different views such as different theories to confirm the interpretation of a phenomenon (Rugg, n.d.). Theory triangulation was not feasible considering the time limitation of the study.

3.2.3.3.4 Methodological triangulation

Methodological triangulation is a process of collecting data using different methods of data collection to measure the same subject through several data collection methods such as interviews, focus groups, observations, and surveys (Rugg, n.d.). These methods can either be multi, mixed, or mono methods. This study adopted data and methodological triangulation where three categories of participants using multi-methods were selected. The multi-methods can be within the same research method (qualitative or quantitative) or across methods (qualitative and quantitative). In this study, the multi-method did not utilise mixed methods but rather methods within the qualitative research. An advantage of using multiple methods is that it produces findings that are more robust and comprehensive when compared to the single method. Kabir (2016) also argues that multiple methods increase the credibility of the findings. Considering the research question for this study, the researcher collected data using multiple methods through an open-ended questionnaire and interviews.

The next layer that needs to be peeled after the methodology choice is the strategy layer which will be discussed in the next section.

3.2.4 Strategy

Research strategy is an overall plan that guides the researcher in executing the study; it informs on how data will be collected and analysed (Creswell, 2018). The choice of the research strategy is influenced by the research questions and objectives, the purpose and the approach, the available body of knowledge, and the available resources (Saunders, Lewis & Thornhill, 2012). The researcher had the option to choose from action research, grounded theory, ethnography, archival research, case study, and survey. These strategies are discussed briefly and defined by Saunders, Lewis, and Thornhill (2007) and Fernandez (2020) as follows:

- Action research is a strategy that intends on closing the gap between research and practice in that a researcher initiates an action to a real organisational problem. This strategy was not appropriate for this study as the emphasis is on what participants are doing than what they are saying based.
- Grounded theory is a strategy used to predict the behaviour of the participants on a specific phenomenon and then develop a theory combining both induction and deduction (Saunders et al., 2007). This strategy can be time-consuming considering the large amount of data it tends to generate. For that reason, this strategy was not feasible for this study.
- Ethnography is a strategy used to understand the social behaviour of a group of people from their natural settings through close observation. This strategy is done over a longitudinal timeframe. Although ethnography may be relevant for this study, the longitudinal timeframe made it not to be relevant for this study.
- As the word archival indicates, archival research requires the researcher to consult historical archives for data collection. For this reason, this strategy was not appropriate for this study.

This study opted for the qualitative survey and the case study as discussed in Sections 3.2.4.1 and 3.2.4.2.

3.2.4.1 Qualitative survey

As indicated by Jansen (2010), qualitative surveys are not defined in the methodological literature although there are studies that may be characterised as using qualitative surveys. Kabir (2016) indicates that the qualitative survey is the study of “diversity” where the researcher aims to get a view and understanding of the subject being studied. Jansen (2010) concurs with Kabir (2016) but argues that this method has not been formally documented. An important aspect to note is that using surveys can be useful in gaining, as well as understanding, the views and opinions of larger samples (Morgan, Rogers-Carter & Christianson, 2017). Qualitative surveys are questions meant to gain extensive information that offers the researchers qualitative information, yet this method seems to be underutilised (Braun, Clarke, Boulton, Davey & McEvoy, 2021). Braun et al., (2021) emphasise that the qualitative survey is underutilised and that there is minimal literature on utilising surveys for qualitative research. Morgan et al., (2017) suggest that the findings from the survey may be followed up by using an in-depth interview to get detailed information on the phenomenon.

The qualitative survey is done through an online questionnaire with open-ended questions. All the participants who agree to take part in this study respond to the survey questionnaire. The benefits of an online survey include a) the cost-effectiveness and convenience of this instrument, b) the development and deployment of the survey are user-friendly and lastly, c) the participants are willing to provide more information in the absence of the interviewer (Morgan et al., 2017). The questionnaire was sent to the participants for them to complete and return it anonymously to ensure confidentiality. Considering that data were collected during the COVID-19 pandemic, the online survey was convenient for both the researcher and the participants. The in-depth interviews were conducted to validate the findings provided by the survey.

3.2.4.2 Case study

Rashid et al*.,* (2019) assert that the purpose of the case study is to conduct intensive research on an identified case which, in this study, is the DWS. Nilmanat and Kurniawan

(2020) argue that a case study can be defined in various ways depending on the purpose it is used for, such as a methodology, strategy, method, and/or approach. Accordingly, a single case study was used owing to its exhaustive nature as it allows for a small sample with various variables that strengthen the understanding of the phenomenon (Rashid et al., 2019). Meşe and Çiğdem (2021) state that case study research is a qualitative approach where the researcher explores an identified case or cases to get in-depth data through multiple sources. The risk management process within the DWS is studied by collecting data through interviews and surveys. According to Rashid et al., (2019), a case study can present the researcher with in-depth knowledge regarding the subject that is being investigated. Creswell and Creswell (2018) assert that a case study involves usually open-ended questions where a researcher gathers views and opinions from the participants through face-to-face interviews.

Conducting research amid a pandemic requires the researcher to have the ability to adapt to different environments (Tremblay et al., 2021). While the interviews are often conducted face-to-face, the COVID-19 pandemic required a change of strategy considering the COVID-19 lockdown regulations. The COVID-19 lockdown regulations promoted the use of technology. In addition, Barrett and Twycross (2018) indicate that during the interview process, participants are encouraged to relay their stories in a narrative form. This allows the participants to voice their views on a phenomenon while the researcher can follow up on some questions for clarity. Barrett and Twycross (2018) view collecting data through interviews as an opportunity to gather rich data and detailed information on the phenomenon being investigated. To gain more detailed information to support and validate the online survey, the interviews were deemed appropriate for this study. The interviews were conducted through Microsoft Teams considering the limitations caused by the COVID-19 pandemic and geographical barriers. The participants were given the option to be recorded with their video on or off for their privacy and comfort.

Utilising an online survey and virtual interviews provided convenience to the study as these two methods provided easy and speedy access to the participants with no travelling costs involved. The researcher took advantage of the ICTs made available.

3.2.5 Time horizon

This layer focuses on the time horizon that the researcher will undertake during the research. Saunders et al., (2019) highlight two types of time horizons namely, cross-sectional and longitudinal horizons.

3.2.5.1 Longitudinal

A longitudinal study is where data are collected over a longer period on repeated occasions with a small sample of the population (Melnikova, 2018). This means that the researcher examines the sequence of events over a phenomenon repeatedly to understand the changes that may occur over a period of time. The longitudinal time horizon is not suitable for this study as the study only intended to collect data once.

3.2.5.2 Cross-sectional

A cross-sectional study applies where the study is going to be conducted in a shorter period and over a specified period, which is the case for this study (Melnikova, 2018). The cross-sectional time horizon is appropriate for this study considering that data were collected once owing to the limited period. The cross-sectional time horizon is exploratory, and it uses either questionnaires or structured interviews to collect data. Some important aspects highlighted by Creswell and Creswell (2018) are that the cross-sectional study allows an examination of how the variables are linked with one another and their ability to determine the frequency of the identified problem. For this study, the intention was to determine how access to ICT resources influences the actual use of these resources in risk management. However, it may not be possible to confirm whether access to ICT resources may result in the effectiveness of the risk management process. It may also be difficult to determine whether the relationship between variables is real. The researcher may not be confident that the use of ICT tools results in the effectiveness of risk management as there is another aspect of the skills that play a role. Yet it can be determined whether using ICT has an effective impact on implementing risk management or not.

The time horizon affects the data collection. The next layer to be peeled is the techniques and procedures used to collect data.

3.2.6 Data collection

Data collection is an important stage of the research study as the type of data a researcher needs to collect influences data collection instruments and the initial research question (Mazhar, Anjum, Anwar & Khan, 2021). Mazhar et al., (2021) define the primary objective of data collection as a process of gathering reliable and valid data for decision-making for the research. There are various research methods that a researcher could choose from, considering whether the research is quantitative or qualitative (Barrett & Twycross, 2018). These methods include surveys, interviews, focus groups, and document analysis. While the COVID-19 pandemic restricted the collection of data using some of the traditional data collection methods, researchers need to strategise and adapt innovative measures such as online data collection (Torrentira, 2020). This minimised the disruptions during the collection of data while considering the lockdown regulations.

The qualitative methodology choice (layer 3 of the research onion) informed the decision of collecting data in this study. Creswell and Creswell (2018) posit that the qualitative data collection methods provide useful information to assist the research with a clear view of the process behind the findings. The researcher collected primary qualitative data in the National DWS using an open-ended questionnaire and interviews. The DWS was selected as the researcher is part of this department where a gap in risk management was identified. For sampling purposes, the researcher considered how the department is geographically located. Figure 3.5 illustrates the business units (based on geographical location) where risk management is implemented in DWS.

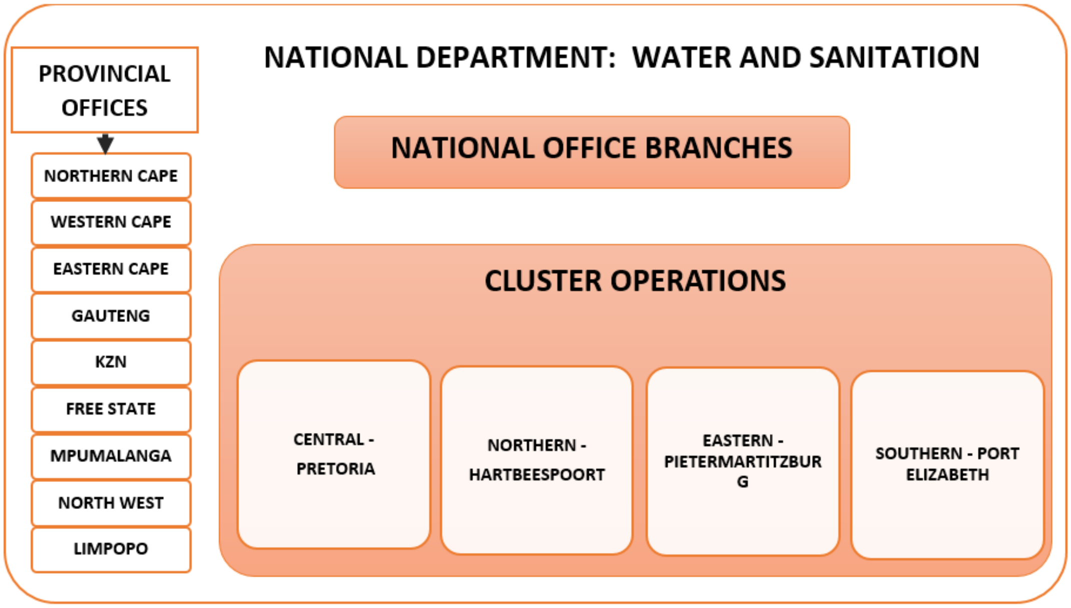


Figure 3.5: Structure and location

The department has a national office in Pretoria as depicted in Figure 3.5. Various branches make up the national office. The department further has offices throughout the nine provinces, namely, Northern Cape, Western Cape, Eastern Cape, Gauteng, KwaZulu Natal (KZN), Free State, Mpumalanga, North West, and Limpopo. There are four cluster offices located in Pretoria – Central Operations, Hartbeespoort – Northern Operations, Pietermaritzburg – Eastern Operations, and Port Elizabeth – Southern Operations.

For data collection to occur, sampling needs to be done. Sampling is a process where participants are selected from an identified population in a fair representation (Creswell & Creswell, 2018). A purposeful sampling strategy was utilised to select the participants to partake in the investigations through the online survey and case study. This decision was informed by the qualitative nature of this study (Creswell & Creswell, 2018). Sampling for this study was also influenced by the availability of resources required for surveys and interviews (Künzli & Gile, 2022). This included whether the participants would have time, knowledge, and access to a network.

3.2.6.1 Survey

The participants were selected based on their role in risk management as well as their years of experience in the field. The total number of participants who qualified to participate in the online survey was 41 and they were categorised as follows:

Five (5) risk practitioners –The risk practitioners are the officials who drive and facilitate the implementation of risk management in the department and are sometimes referred to as the risk management team in the study. The risk practitioners are categorised into two groupings, the deputy directors who are sub-unit heads, and the risk practitioners who support these deputy directors. The risk practitioners are the custodians of the risk management process in the department. Some of their responsibilities include the implementation of risk management in the department, providing support to the risk champions and the risk owners, ensuring the use of technology to support the implementation of risk management, and providing training and awareness to the department.

Thirty-one (31) risk champions – these are key officials who coordinate risk management activities within various areas (eighteen from head offices in Pretoria, nine from the regional offices in the nine provinces, and four from the cluster offices located in Pietermaritzburg, Port Elizabeth, Hartbeespoort, and Pretoria). These officials work closely with the risk practitioners. The risk champions coordinate risk management activities in their respective business units. The risk champion facilitates the risk assessment and the monitoring of the risk mitigations, capture and monitors the progress of the identified risks on the system, prepares risk management reports for the risk committee meetings, and conducts risk awareness.

Five IT officials provide IT services to the department. Among these participants, some of them are risk owners in their specific areas. Risk owners play an overall responsibility for implementing risk management in their business units with the assistance of the risk champions.

The researcher assigned codes to each participant for the anonymity of the participants. In this way, the details of the participant remain confidential throughout the study. For the qualitative survey, participants from 1 to 30 were given a code starting from 01 and ending at 30 regardless of the role they played.

3.2.6.2 Case study

Out of the total number of participants who were sampled for the survey, only ten officials were selected to participate in the interviews. These participants were selected based on their activeness in implementing risk management in the department and their experiences. While there were many officials tasked to support the implementation of risk management (risk champions and practitioners), some of the risk champions were not actively involved in the process. Furthermore, these participants were selected as they were available throughout the study. These participants included the five risk practitioners and the five risk champions. The participants were allocated letters from A to I irrespective of the role they played in risk management. The participants were divided into three categories according to age groups as age is a contributing factor to ICT adoption. The age group categories intended to understand whether participants from various age groups embrace technology differently.

3.2.6.3 Instrument development and distribution

Oben (2021:p 2) refers to a research instrument as a “scientific and systematic” tool that is developed to collect, evaluate, and analyse data to answer the research question. The researcher develops or selects an instrument appropriate to the research study being conducted, in this case, an instrument for collecting qualitative data (Creswell & Creswell, 2018). For this study, the first instrument developed was an online survey. An open-ended survey was developed using Google Forms, which was then distributed using email and WhatsApp where there was no access to email. The questionnaire (survey) was divided into four categories (Appendix F), general and professional information, and the other three categories aligned with the research questions. An online survey allows the researcher to distribute the questionnaire to the participants through an online platform (Torrentira & Moises, 2020). While this instrument provided conveniences in terms of access to several participants, it was feasible considering the COVID-19 lockdown regulations. The online survey was easily sent to all the participants with a high number of responses from the participants.

Secondly, the interview questionnaire was developed with pre-determined structured questions. Face-to-face interviews are the most common data collection technique; however, the interview questionnaire was designed to allow either face-to-face or virtual interviews. Considering that data collection took place during October and December 2020, which was when the country was under COVID-19 lockdown regulations, it was not possible to conduct face-to-face interviews. The adaptive approach of collecting data was utilised, where interviews were done virtually using Microsoft Teams.

3.2.7 Data analysis

Data analysis is the process of examining the data collected from the participants to answer the research questions raised in a study (Sharma, 2018). The key elements of this process include the identification of themes or patterns, determining suitable data, selecting an appropriate data analysis method to get to the recommendations, and the conclusion of the study. As this study collected qualitative data through an open-ended survey and interviews, the qualitative data analysis method was selected. According to Adu (2019), qualitative data analysis (QDA) is the process of analysing data for understanding where the researcher moves from the collected qualitative data to explanations, understanding, and interpreting what the participants are saying about the subject being investigated. This is to ensure that, for the researcher to get to the conclusion of the study, the perceptions of the participants are clearly defined and interpreted to get informed recommendations.

Maxwell (2018) highlights and defines the common types of qualitative data analysis such as content analysis. Content analysis is used to categorise data in various classes based on various themes identified from the collected data. Roller (2019) maintains that content analysis does not collect data from people. Furthermore, content analysis has some form of quantification of data that is not relevant to this study. The second data analysis is the narrative analysis which is used to interpret everyday stories in a context of a research study at hand. The meaning of these is constructed through negotiation and collaboration between the participant and the researcher. Thirdly, in discourse analysis, the researcher analyses the verbal interactions and any written text from the participants focusing on how participants express themselves. Fourthly, the grounded theory allows the researcher to examine the first case of the population to formulate a theory and later additional cases can be examined to determine their contribution to theory formulation. While some of these tools may be appropriate for this study, such as content and narrative analysis, the analysis tool that was the most suitable for this study was thematic analysis.

3.2.7.1 Thematic analysis

Thematic analysis is used to identify themes from the data collected from various participants. These themes were used to code for the purpose of interpreting the findings (Braun & Clarke, 2006). While thematic analysis originated in the early 1970s by Gerald Holton, it has not been fully claimed as an analysis method like grounded theory among many analysis tools (Braun & Clarke, 2006). However, thematic analysis has developed over the years and started being acknowledged as a distinctive method with a clear approach to analyse data (Clarke & Braun, 2013). The thematic analysis was selected for its flexibility to analyse any kind of qualitative data such as focus group interviews. Furthermore, the thematic analysis provides the adaptability that allows the researcher to present and analyse data through themes. According to Clarke and Braun (2013), thematic analysis provides steps that are user-friendly for data analysis.

The data from both the survey and the case study were analysed using thematic analysis. Robinson (2022) suggests that thematic analysis is best presented and conducted using Microsoft Excel. This format allows ease of identifying, analysing, and reporting themes, including interpreting various aspects of the investigated topic (Braun & Clark, 2006, p8). To report on this thematic analysis, tables, graphs, and a detailed discussion on how thematic analysis was used for this study were done in the analysis chapter (Chapter 4). The researcher must ensure that the data collected and analysed is trustworthy. The next section presents the validity and reliability of the data.

3.3 MEASURING THE TRUSTWORTHINESS OF THE STUDY

Trustworthiness is defined as the level of confidence that the readers have in data, interpretation, and methods used in the study (Polit & Beck, 2017). As indicated in the study conducted by Gunawan (2015), a research study can only be trustworthy if the reader believes it to be trustworthy.

3.3.1 Credibility

To determine credibility, the researcher used the lens from the researcher’s view to ensure that relevant and good themes would be established from the collected data. This is where data from both the survey and interviews were repeatedly engaged. To further evaluate data from the interviews, detailed transcription from the video and audio recordings was done.

Furthermore, the researcher ensured that the findings were compatible with reality and trustworthy. This was done through triangulation where the data set from the survey was validated against the data set from the interviews. The use of different data sources methods such as interviews and surveys allowed the researcher to determine consistency in the findings (Korstjens & Moser, 2017). In cases where required, multiple interviews were conducted for the verification of consistency. Moreover, the process of triangulation ensured the reliability of the findings (Hayashi, Abib & Hoppen, 2019). The use of two data collection methods for different groups of participants assisted to determine consistency and reliability (Hayashi, Abib & Hoppen, 2019). Hammarberg, Kirkman, and Lacey (2016) argue that consistency can only be achieved if the other research finds comparable results given the same data in a different context.

3.3.2 Objectivity

Zahle (2021) argues, regarding objectivity in research support, that research justification can only be objective when it is not influenced by non-epistemic values. To determine objectivity in research, various features that contribute to objectivity should be considered (van Dongen & Sikorski, 2021). To ensure objectivity in this study, the researcher ensured that data were accurately described to demonstrate exactly what the participants indicated during interviews either verbally or non-verbally. This was done with the assistance of the transcription and interview notes that were taken during the interviews. Furthermore, the only data that were used were data from the interviews related to the research objectives which had the potential to satisfy the research questions posed.

3.4 ETHICAL CONSIDERATIONS

Ethical considerations are crucial for research, especially when human subjects are involved (Arifin, 2018). According to Haines (2017), researchers need to be considerate of any ethical issues relating to the research topic, participants, design, and collection of data. Ethical considerations in this study were guided by the Unisa research policy. Permission was requested and approved to conduct the research in the DWS. In line with the Unisa research policy, an ethical clearance application was done to the Unisa Ethics Committee before data collection. The ethical clearance aimed to ensure that the researcher maintains confidentiality and privacy for any participants in this study. Once the ethics clearance certificate (Appendix C) was granted by the research committee of the School of Computing (SoC) at Unisa, the participants were requested to partake in the study. The information pack (Appendix D) was provided to the participants together with consent forms (Appendix E) for completion by those who agreed to participate.

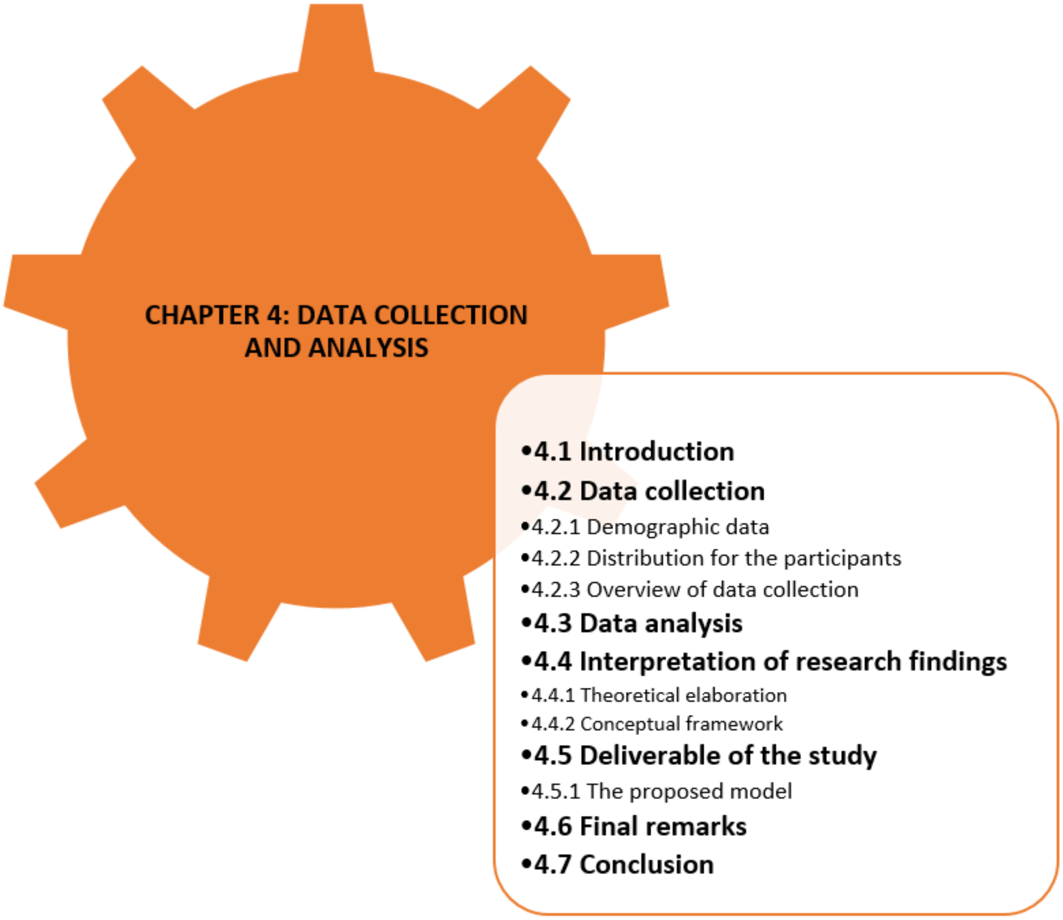
Considering the COVID-19 pandemic that the country and the world were facing in 2020, the researcher ensured compliance with the rules and regulations in line with COVID-19. While face-to-face interviews were planned, this was not possible during the lockdown owing to social distancing measures. The researcher opted for safer data collection methods where interviews were conducted using virtual connections and online surveys for the safety of participants and the researcher.

3.5 CONCLUSION

This chapter described the research methodology adopted in this study focusing on the research design and philosophy. This chapter discussed all the components of the research design including the research methods, data collection and analysis, and validity and trustworthiness. As the collection and analysis of data require compliance with ethical considerations, this chapter also gave a brief description on how the process of ensuring ethical compliance was done. The results will be presented and discussed in the next chapter.

CHAPTER 4: DATA COLLECTION AND ANALYSIS

This chapter presents an outline of the analysis of the collected data and the proposal of the model that forms part of the study's deliverable. The layout of this chapter is presented in Figure 4.1. This chapter outlines the introduction in Section 4.1, the data collection in Section 4.2, analysis of the research findings in Section 4.3, and the deliverable of the study that proposed the model for the integration of ICT to support risk management in Section 4.4. Lastly, final remarks are presented in Section 4.5 with the conclusion in Section 4.6.



CHAPTER 4: DATA COLLECTION AND ANALYSIS
•4.1 Introduction
•4.2 Data collection
•4.2.1 Demographic data
•4.2.2 Distribution for the participants
•4.2.3 Overview of data collection
•4.3 Data analysis
•4.4 Interpretation of research findings
•4.4.1 Theoretical elaboration
•4.4.2 Conceptual framework
•4.5 Deliverable of the study
•4.5.1 The proposed model
•4.6 Final remarks
•4.7 Conclusion

Figure 4.1: Chapter 4 layout

4.1 INTRODUCTION

The previous chapter outlined the research methodology adopted in this study. This chapter focuses on data collection and analysis. The data were gathered through a qualitative online survey using a questionnaire and interviews using Microsoft Teams. The main research objective as presented in Section 1.4.1 of this study is to determine whether the use of ICT to implement risk management has an impact on the effectiveness of risk management. The sub-objectives supported the main research objectives. The overall intention of this study is to propose a model to integrate ICT in risk management as indicated in Section 1.7. The research questions were answered through the qualitative survey and interviews where the participants, as outlined in the next section, participated. Section 4.2 discusses data collection.

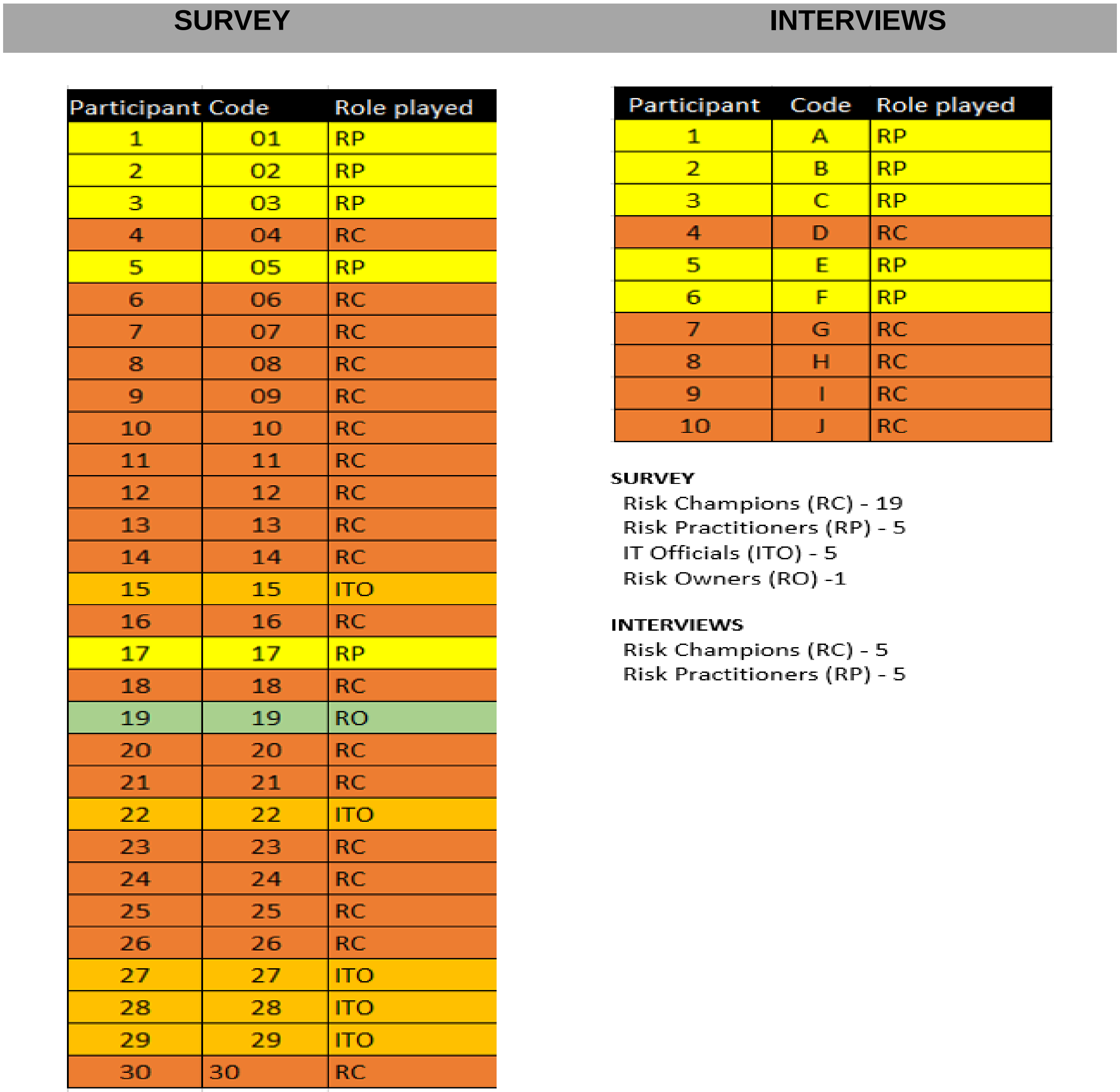
4.2 DATA COLLECTION

This study focused on collecting data relevant to the use of ICT in risk management within the public sector. As such, data were collected from the participants who were key in the implementation of risk management in the public sector. Prior to data collection, the information pack and the consent forms were sent to the 41 participants (Appendix E). The information pack provided the participants with the background and what was expected of them while the consent form was for them to complete as confirmation for their participation in the study. Out of the 41 participants, only 30 responded. Most of the consent forms were not returned to the researcher prior to the data collection owing to connection challenges as this was during the COVID-19 lockdown period. The participants, however, confirmed their participation through WhatsApp committing to submitting the consent forms once they returned to their offices, which was done.

Data collection methods were discussed in Section 3.2.6 where qualitative data were gathered through the survey and interviews. Section 4.2.1 discusses the demographic data for the participants.

4.2.1 Demographic data for the participants

The participants were divided into four categories such as risk owners, risk practitioners and risk champions and IT officials based on the roles they played in risk management, as illustrated in Figure 4.2.



SURVEY

Participant	Code	Role played
1	01	RP
2	02	RP
3	03	RP
4	04	RC
5	05	RP
6	06	RC
7	07	RC
8	08	RC
9	09	RC
10	10	RC
11	11	RC
12	12	RC
13	13	RC
14	14	RC
15	15	ITO
16	16	RC
17	17	RP
18	18	RC
19	19	RO
20	20	RC
21	21	RC
22	22	ITO
23	23	RC
24	24	RC
25	25	RC
26	26	RC
27	27	ITO
28	28	ITO
29	29	ITO
30	30	RC

INTERVIEWS

Participant	Code	Role played
1	A	RP
2	B	RP
3	C	RP
4	D	RC
5	E	RP
6	F	RP
7	G	RC
8	H	RC
9	I	RC
10	J	RC

SURVEY

Risk Champions (RC) - 19
Risk Practitioners (RP) - 5
IT Officials (ITO) - 5
Risk Owners (RO) -1

INTERVIEWS

Risk Champions (RC) - 5
Risk Practitioners (RP) - 5

Figure 4.2: Description of participants

These roles were defined in Section 3.2.6.1. The total number of survey participants was 30. This number was made of 19 risk champions, five risk practitioners, five IT officials, and one risk owner. The participants for the interviews were ten, five risk champions, and 5 risk practitioners. The interview participants were part of the 30 participants. These participants were differentiated using the code for the survey as numbers 01 to 30 while, for the interview participants, letters from A to J were used. Section 3.2.6 provided detailed information on the participants, such as the business units they represented. Section 4.2.2 discusses how the participants were distributed.

4.2.2 Distribution of the participants

The officials who participated in this study were distributed across the DWS according to the structural and functional arrangements of the organisation. Table 4.1 illustrates how the participants were distributed.

Table 4.1: Distribution of participants

AGE GROUP	NUMBER OF PARTICIPANTS	COMPOSITION
25 - 35	5 (16.5%)	2 Risk Practitioners, 2 Risk Champions, and 1 IT official
36 - 46	20 (67%)	3 Risk Practitioners, 13 Risk Champions and 4 IT officials
47 - 60	5 (16.5%)	4 Risk Champions, 1 Risk Owner

Table 4.1 provides the age groups, the number with a percentage, and the composition of participants. The total number of participants in the table is 30. There were 5 participants in the youngest group (25 to 35), 20 were in the middle group (36 to 46) and the last 5 were in the eldest age (47 to 60) category. The qualifications of the participants are not included in the table as they vary across the age groups and the composition groups. The qualifications range between diploma to master’s level in various disciplines. The participants were composed of 5 directors, 13 deputy directors, 10 assistant directors, and 2 risk practitioners structurally. While Table 4.1 refers to the 5 risk practitioners, these practitioners are appointed on various levels such as deputy directors and risk practitioners. The IT officials were at various levels with the highest level being

a director. There were 5 directors appointed as risk champions in their respective offices. These participants formed part of the age group that ranges between 47 and 60. The various business units decide on the official that they want to appoint as the risk champion in terms of the levels. The levels for the risk practitioners, IT support and risk owners are determined by the business unit structure. A new role emerged during the data analysis process where one risk champion converted to being a risk owner owing to the change of responsibilities. Table 4.2 illustrates a data collection overview.

4.2.3 Overview of data collection

An overview of the data collection is illustrated in Table 4.2 focusing on the strategy adopted, the number of participants for each strategy, the sites and dates where data collection was conducted, the duration and the instruments utilised, and lastly, the role played by the researcher in data collection.

Table 4.2: Data collection overview

DATA COLLECTION STRATEGY	NUMBER OF PARTICI-PANTS	SITE AND DATES	DURATION	RESEARCH INSTRUMENT	ROLE OF THE RESEARCHER
Survey	30 (Risk Practitioners, Risk Champions, and IT officials)	DWS 23 October to 11 November 2020	19 days	Online questionnaire (open-ended)	Administer the survey
Case study	10 (Risk Practitioners and Risk Champions)	DWS 12 to 23 November 2020	12 days	Interviews (Microsoft team and smartphone for backup)	Interviewer and record taker

The first strategy to be discussed is the survey (Appendix F).

4.2.3.1 Survey

An online qualitative survey was done with 30 participants from national, regional, and cluster offices. After the participants confirmed their participation in the study, a predetermined questionnaire was developed and sent to the sampled participants on 23 October 2020. The questionnaire was structured into four main categories, namely, general information about the participant and their professional experience, access, and use of Information Communication Technology (ICT) in risk management, attitude of the users towards using ICT in risk management, and the challenges experienced by the users in using ICT (Appendix F). The participants completed and returned all the questionnaires by 11 November 2020. The completion and submission of the online questionnaire took about 19 days.

4.2.3.2 Case study

To confirm and validate the results of the survey, interviews were arranged with the ten participants as illustrated in Table 4.2. The interviews were conducted from 12 to 23 November 2020 using the pre-determined interview questions (Annexure G). The questions for the interviews were designed to align with the survey questions as the interviews were intended to validate the survey. Yet the interview questions were influenced by the research objectives. To avoid inconveniencing the participants, the interview schedule was also developed to allow proper planning. The interview process lasted for 12 days. The interviews were video or audio recorded for validity evaluation during the analysis of data. The notes were also documented to assist in analysing data.

4.3 DATA ANALYSIS

The analysis of data was done using the thematic analysis for both the survey and the case study as discussed in Chapter 3. Figure 4.3 illustrates the steps taken to analyse the data collected. These steps followed a six-phased approach to thematic analysis (Labra, Castro, Wright and Chamblás, 2020).

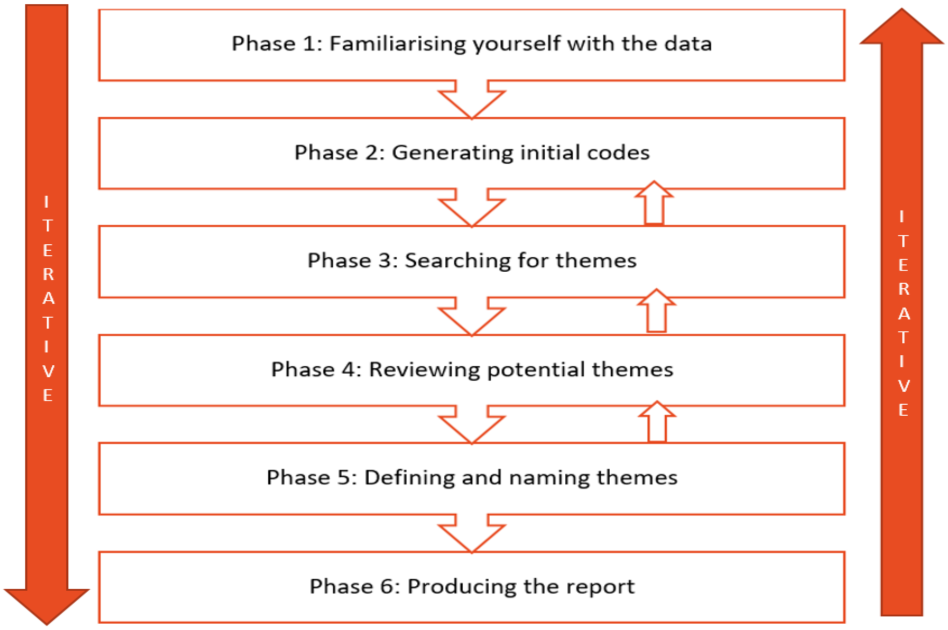

Phase 1: Familiarising yourself with the data
Phase 2: Generating initial codes
Phase 3: Searching for themes
Phase 4: Reviewing potential themes
Phase 5: Defining and naming themes
Phase 6: Producing the report
ITERATIVE
ITERATIVE

Figure 4.3: Thematic analysis

Sources: Labra et al. (2020)

The next section discusses how thematic analysis was used for the survey followed by the case study. While both the survey and case study data were analysed following the same steps of thematic analysis, the data from the case study were only analysed after the survey was concluded. This process was done to validate the results of the survey. However, the discussion for each step commences with the survey followed by the interviews for each phase. Table 4.3 illustrates phase one of the thematic analysis for the survey. The three participants used in each phase were randomly selected for presentation. Section 4.3.1 discusses phase one of the thematic analysis.

4.3.1 Familiarisation with collected data

For phase 1, an Excel template was developed based on the questions asked in the survey questionnaire and the number of respondents who responded as illustrated in Table 4.3. The table illustrates the subject questions in line with the questions asked on the survey, with responses from each respondent for each subject question.

Table 4.3: Phase 1 – Familiarize with data survey

REPRESENTATION OF RESPONDENTS 1 TO 30			
Subject question	**RC - 01**	**RP - 02**	**RP - 03**
Equipment	Laptop	Desktop, Laptop, Smartphone	Laptop, Smartphone
Frequency of using the ICT resources	Word- 1, excel 1, teams 1, sap 2, PowerPoint 2,	Word- 1, excel 1, teams 1, sap 1, PowerPoint 1,	Word- 1, excel 1, teams 2, sap 1, PowerPoint 4
ICT skills	N-drive 3, SAP 3, Internet 4, Teams 3, PowerPoint 3,	N-drive 4, SAP 5, Internet 5, Teams 4, PowerPoint 4,	N-drive 3, SAP 3, Internet 3, Teams 3, PowerPoint 3,
Purpose of ICT resource	Word-Reporting, PowerPoint - presentation, email - communication, internet - researching, and teams - meetings	Word -Memo, PowerPoint - presentation, email - conveying messages, internet - researching and teams -meetings	PowerPoint - Presentation Ms team - Meeting Internet explorer- GRC system Ms word - report writing
Reasons for not using the ICT resource	All resources are used	All resources are used	No limitation, all the ICT resources are in use
Significance of using the ICT resource	Strongly Agree	Strongly Agree	Strongly Agree
Usefulness of the ICT resource	Agree	Strongly Agree	Strongly Agree
The challenges affecting the use of ICT in risk management within the department?	The system can be slow at time	Lack of skills, being computer literate and not be able adapting to change (Technological enhancement)	NULL (no response provided)
Measures to address the challenges in risk management within the department	Communicate with IT and system owners where there are challenges	Regular training and awareness on ICT	ICT training improve network accessibility

REPRESENTATION OF RESPONDENTS 1 TO 30			
Subject question	**RC - 01**	**RP - 02**	**RP - 03**
Benefits of addressing these challenges?	To enable users to access the system easily	All officials will be able to access and use the IT systems. There will be ease reporting the changes/development in the technological environment will be applied in the organisation	Improved the overall organisational performance

When the respondents submitted their questionnaires, data were captured on the analysis process template. This assisted the researcher to ensure that accurate and reliable data were maintained. For confidentiality, each respondent returned the questionnaire anonymously through the online platform. Each respondent was allocated a code from 1 to 30 to adhere to anonymity. Furthermore, a code was allocated to each respondent for the role they played such as RC (Risk Champion), RP (Risk Practitioner), RO (Risk Owner), and IT (Information Technology official). The data collected from the survey was captured against each question. When all the questionnaires were submitted, the initial analysis of data commenced. Appendix I provides only a snapshot or a sample of the template considering the size of the data captured.

After the themes were defined and named from the survey, a template like the one for the survey was developed to capture the raw data from each of the interviewed participants as illustrated in Table 4.4. The table illustrates the questions asked for each interview participant, with responses for each question. For anonymity, each participant was allocated a code from A to J. Table 4.4 only provides a sample of participants A to C for demonstration purposes. The researcher retrieved the recorded interview videos and audio to prepare for the analysis process. The transcripts done during the interviews were also retrieved. The raw data informed by the transcripts for each participant were captured (and reviewed) based on the question asked during the interview for ease of analysis (Appendix N). After capturing data elicited from the participants, the researcher engaged the data to get a better understanding of the data. This assisted with the identification of noticeable patterns, getting the feelings from the voices of the participants among other things.

Table 4.4: Phase 1 - Familiarise with data – Interviews

REPRESENTATION OF SAMPLED PARTICIPANT A TO J				
QUESTION		RP - A	RC - B	RP - C
1	Tell me about your role in risk management.	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy, and strategy.	I am currently a Risk Practitioner and my role there is to facilitate the risk management processes by making sure that we manage our risks in the organisation well and being monitored and reported.
2	Do you have access to any ICT tools e.g., computer, system, internet etc?	Yes, I do. Laptop system (SAP) Ms office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cell phone, emails, teams, zoom and SAP GRC system	Yes, we do have. I do have the laptop; the system we call SAP that we use to capture our risks. We access internet, emails, I can say we do have all the ICT tools. And we do have teams.
3	How do you use ICT tools in your daily risk management activities?	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk registers on pull up reports – all types of reports for various purposes, quarterly reports. Monitoring the status. SAP administrators, outsourced system. Risk owners, Risk champions and risk practitioners. RC assist the risk practitioners to update the system, can identify the risks through the system. System	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC system. When I am doing risk forums and any other meetings – I am using power point presentations as it makes it easy to engage my stakeholders through teams, During the COVID 19 period, I use of virtual meetings through Ms Teams. During this period, we needed to roll out the	With the laptop, everything we are capturing on the laptop. It's our working tool this one. And then even the system we are using it on the daily basis by going into that system whereby we capture our risk, retrieve the report. And everything that is needed in terms of our risks because it is a daily thing. And even the email, we communicate with the email more often We use internet even to access our system. MS teams also is a daily thing, even now with this thing since even now we are faced with this thing of COVID so for us to

REPRESENTATION OF SAMPLED PARTICIPANT A TO J				
		monitored by the risk practitioners.	Risk Appetite and Tolerance framework. For the implementation of Risk Appetite T videos were used to create awareness on the framework.	have meetings we are using teams. I can say we use them on daily basis. Having these ICT tools is very helpful.
4	Is ICT playing an effective role in implementing risk management activities	I would not say effective, but they are playing a role. Currently the assessment is done manually however the system is capable to do assessment. To avoid duplicate, preference would be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	Yes. The reason I am saying yes is that it makes things easy. We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	What I can say is that it plays a major role, my answer is YES. In us for example, for us to work we need IT. Even with our system whereby we capture everything pertaining to our work. It becomes easy when it comes to reporting because we even receive the reports from that particular system unlike when using manual. The issue of the meetings, we do need cases where we need to go to meet in one room but with this ICT tool teams, it’s easy to just log in on teams and we have our meeting.

In preparation for phase 2, the researcher engaged the raw data to ensure the understanding of the messages provided by the participants. To keep a record of some useful messages that emerged from the data, notes were made. This led to Section 4.3.2, where initial codes for the survey were generated.

4.3.2 Generate initial codes

During phase 2, the researcher started the coding process for the survey by highlighting sentences that have commonalities as indicated in Table 4.5.

Table 4.5: Phase 2 – Generate initial codes - Survey

REPRESENTATION OF RESPONDENT 1 TO 30				
Subject question		**RC - 4**	**RP - 5**	**RC - 6**
Access to ICT resources	**Equipment**	Laptop, Smartphone	Laptop	Laptop, Smartphone
	Resource	Network drive, IT System (SAP GRC), Internet Ms Teams/ Zoom	Network drive, IT System (SAP GRC), Internet, Ms Teams/	Network drive, Internet, Ms Teams/ Zoom
Usefulness of ICT resources				
Frequency of using the ICT resources		Word- 1, excel 1, teams 2, sap 4, PowerPoint 3	Word- 1, excel 2, teams 2, sap 2, PowerPoint 3	Word- 1, excel 1, teams 1, sap NULL, PowerPoint 4
ICT skills		N-drive 2, SAP 2, Internet 3, Teams 2, PowerPoint 3,	N-drive 3, SAP 3, Internet 3, Teams 3, PowerPoint 3,	N-drive 4, SAP NULL, Internet 4, Teams 3, PowerPoint 4,
Purpose of ICT resource		to be able to fulfil my work duties	I use them to do my work	no answer
Reasons for not using the ICT resource		I am using them	I use them	I use them all
Significance of using the ICT resource		Strongly Agree	Agree	Strongly Agree
	Usefulness of the ICT resource	Agree	Disagree	Strongly Agree
Impact of ICT	**Identification and assessment process**	Strongly Agree	Agree	Strongly Agree
	Reporting of risks	Agree	Disagree	Strongly Agree

These commonalities were organised to reduce data that were not relevant. This was done considering the research question that the study had intended to achieve. This allowed the researcher to generate initial codes to prepare for phase 3. The initial codes are presented in Appendix J1 to J2. Following the initial codes, themes from the survey were searched as discussed in Section 4.3.3.

Following step 2 of the interview analysis, the researcher started the coding process by highlighting areas with commonalities as illustrated in Table 4.6. An interesting thing with this process was that the emerging patterns confirmed the patterns identified from the survey.

Table 4.6: Phase 2 – Generate initial codes – Interviews

QUESTION		RP- A	RC-B	RP-C
1.	Tell me about your role in risk management.	It's not my responsibility nor my role I am just assisting because there is no dedicated official for compliance and risk management. That on its own result in the function not being performed religiously because e there is no dedication function for risk because my responsibility is to just coordinate risk. Not necessarily that see to it that all the advice and recommendations from risk management team are implemented. And what needs to be done in order to address certain problems in certain areas. As long as I get the reports, that's honeymoon. Because I am not an expert in the field. Am just coordinating the reports	I am Deputy Director responsible to facilitate the implementation risk management in the department.	My role as a risk practitioner is assist the risk management team in terms of implementing the risk management process within the department in a way of monitoring our risk processes on a quarterly basis…. like monitoring the risk reporting and the risk registers. And also, I assist with the awareness processes where we conduct awareness to instil the culture of risk management, I also do administrative work in terms of our committees – prepare for arranging logistics for the risk management committees. Overall, I can say I assist in implementing the risk management processes in the department.
2.	Is ICT playing an effective role in implementing risk	I would not say effective, but ICT is playing a role. Currently the assessment is done manually however the system is capable to	Yes The reason I am saying yes is that it makes things easy.	What I can say is that it plays a major role, my answer is YES. As risk management I can say meeting is a daily thing because we meet with various stakeholders so even

QUESTION		RP- A	RC-B	RP-C
	management activities	do assessment. To avoid duplicate, preference would be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	if we don't talk to them via meetings, the email we get from ICT we are able to communicate via email and do what we want as risk management. So really ICT plays a major role in our activities, without it we may not survive. During the period of COVID 19We even did…for example as risk management we sometimes roll out things like the new processes, the new framework that we develop. We used this ICT to roll out our framework whereby we did the presentation and recording…rolling out of framework to all our stakeholders virtually and throughout the department via email and the cell phone – WhatsApp. Even this issue of meeting…. we were having our meetings as usual using Ms team. It really assisted us

The first question on the participant's role, however, provided a new pattern that talked to the implementation and facilitation of risk management framework, policy, and process. This pattern was deemed critical for the development of the proposed model for this study.

The initial codes are presented in Appendix J3. The next phase was to search for themes as discussed in the next section.

4.3.3 Search for themes

In phase 3, the themes for the survey were searched based on the colour-coded sentences done during phase 2 as illustrated in Table 4.7.

Table 4.7: Phase 3 – Search themes - Survey

REPRESENTATION OF 1 TO 30 PARTICIPANTS		
RC - 01	**RP - 02**	**RP - 03**
Slowness in SAP system makes it difficult to upload PoE.	availability of technology, training and adoption of risk management tools	No access to data when officials are working from home
The SAP system must be improved for efficiency and effectiveness.	communication of importance of risk management, training, ensuring up-to-date IT infrastructure	Officials need to be provided with working tools like data even when working from home
Reporting will be done effectively.	it will be easier for employees to report and manage risks within the environment	Better communication and timeous reporting in Risk management and other activities

The researcher reviewed the identified codes and engaged them linking the relevant codes to the research question. This formed a first level of themes that required to be reduced further (Appendix K). This process was moved to a different sheet to differentiate the key themes from the extensive list of themes. The colour-coded themes that were irrelevant based on the frequent codes to the dataset were discarded. Phase 3 for the interviews followed the same process for the questionnaire as illustrated in Table 4.8. The first level of themes that required to be reduced further is illustrated in Appendix O.

For ease of reference, the color coding legend for the themes is as follows:

Access to resources	⬜
Usefulness of the ICT resource	🟩
Impact of the ICT resource	🟦

Table 4.8: Phase 3 - Search for themes – Interviews

Subject question	RC - 01	RP - 02	RP - 03
Framework for risk management - to inform the model/ proposed framework	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy and strategy.	My role there is to facilitate the risk management processes by making sure that we manage our risks in the organisation well and being monitored and reported.
Access to resources to resource	Yes, I do Laptop system (SAP) MS office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cell phone, emails, teams, zoom and SAP GRC system	Yes, we do have. I do have the laptop, the system we call SAP that we use to capture our risks. We access internet, emails, I can say we do have all the ICT tools. And we do have teams.
Usefulness	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk registers on pull up reports – all types of reports for various purposes, quarterly reports. Monitoring the status. SAP administrators, outsourced system. RC assist the risk practitioners to update the system, are able to identify the risks through the system.	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC system. When I am doing risk forums and any other meetings – I am using power point presentations as it makes it easy to engage my stakeholders through teams,	... And then even the system we are using it on the daily basis by going into that system whereby we capture our risk, retrieve the report. … we communicate with the email more often We use internet even to access our system. MS teams also is a daily thing, even now with this thing since even now we are faced with this thing of COVID so for us to have meetings we are using teams. I can say we use them on

Subject question	RC - 01	RP - 02	RP - 03
	System monitored by the risk practitioners.	During the COVID 19 period, I use of virtual meetings through Ms Teams.… implementation of Risk Appetite videos were used to create awareness on the framework.	daily basis. Having these ICT tools is very helpful.
Impact of ICT resources	I would not say effective, but ICT is playing a role. Currently the assessment is done manually however the system is capable to do assessment. To avoid duplicate, preference would be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	Yes. The reason I am saying yes is that it makes things easy. We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	What I can say is that it plays a major role, my answer is YES. So really ICT plays a major role in our activities, without it we may not survive. During the period of COVID 19 We even did…for example as risk management we sometimes roll out things like the new processes, the new framework that we develop. We used this ICT to roll out our framework whereby we did the presentation and recording…rolling out of framework to all our stakeholders virtually and throughout the department via email and the cell phone – WhatsApp. Even with the issue of meeting, we were having our meetings as usual using Ms team. It really assisted us a lot during COVID 19.the usage of ICT

3.4 Review themes

In phase 4, data were further engaged to reduce the data further as illustrated in Table 4.9 for the survey (Appendix L). The key themes that were most relevant to answer the research question were identified. This process resulted in the raw data being reviewed, and patterns and themes further identified. Notes were also made on the side to identify areas that had a potential for clarification.

Table 4.9: Phase 4 – Review themes – Survey

Resources	*Skills - usefulness*	*Effective reporting/ accessibility - impact*	*Resources*	*Training*
Lack of consistent training of all risk owners and champions	limited/ lack of ICT skills, being computer literate,	Not using the ICT reporting system daily can affect the effectiveness of reporting.	Lack of resources including laptops (aging laptops or desktops) - unable to work especially remotely and slow implementation of ICT projects.	Ignorance from risk owners and managers.
Inadequate and inefficient availability of ICT resources	Lack of dedicated risk practitioners in departments and divisions	The amount of time it takes to use the system	Efficient use of the systems	The level of appreciation of the ICT Risk management is still low among other line function managers resulting in some case having to revert back Excel type of reporting.

For the interviews, data were further engaged to make sense of the preliminary themes as illustrated in Table 4.10 (Appendix P). The same process was done for the survey to identify the key themes was done for interviews. Beyond the interview being recorded, the notes were documented to assist in analysing data. This assisted in giving the full view of what participants felt about the use of ICT in risk management and how it impacts them. This allowed the researcher to be familiar with the collected data. Furthermore, this allowed easy reduction of the collected data by capturing what was relevant.

Table 4.10: Phase 4 Review themes – Interviews

Subject question	Resource	Usefulness	Impact
1. Access to equipment and resources 2. The challenges affecting the use of ICT in risk management within the department. 3. Measures to address the challenges in risk management within the department 4. Benefits of addressing these challenges?	Resource allocation	Skills	Effective reporting/ accessibility
	Access to system	Education and awareness	Ease access/ use of system
	Infrastructure	Training and awareness	Efficiency
	Technology/ infrastructure	Creating ICT culture	Communication
	Resources		Potential to improve,
			Positive impact

This process resulted in the mapping of the codes to the preliminary themes as illustrated in the thematic map in Table 4.11 that informed the themes defined in Section 4.3.5.

Table 4.11: Thematic Map

THEME	CATEGORY	CODE	CATEGORY	CODE
	Survey		Interviews	
Access to ICT resources (Section 2)	ICT tools and equipment made available	Ms Office, shared network drive, laptop, virtual platforms, IT system, phones access, down times, slow system, network access, aging, availability	Access to ICT tools Role of the participant	Ms Office, shared network drive, laptop, virtual platforms, IT system, phones access, inability to access, remote access, slow system implementing the frameworks, facilitate risk management processes, coordinate
	Access to ICT tools and equipment	unreliable, interruption, ineffective, inefficient, inadequate, slow	Access to ICT tools	system tired while capturing, system requires a lot of data, network issues
Usefulness of the ICT resource (Section 2)	Skills competency	efficient, computer literate, lack of adapting, change, ICT skills, knowledge	Use of ICT tools, ICT challenges	lack of understanding, reluctance to change, shortage of resources, skills and capacity
Impact of ICT (Section 3)	The importance and usefulness of the ICT tools	infrastructure, effective efficient, prioritized, budget/ funding	Future of ICT	major role, very helpful, effective role, effective, do away with the manual, makes things easy
	Perceived impact of ICT on risk management		Future of ICT, Additional information	enhance productivity and communication, life easy, save time

4.3.5 Define and name themes

From the thematic map in Table 4.11, the key themes were defined and named to provide the essence of what each theme represents and given the relevant names in line with what the study intended to achieve (Appendix M and Q). The themes that emerged from the interviews confirmed the three themes from the survey data. The areas that needed clarity from the survey were followed up through the relevant questions from the interviews. The critical question that the survey missed was on the IT risk assessment being conducted in the organisation. While it was indicated that the risk assessments were conducted at a strategic level which was done at the National Office level, the approach followed for the IT risk assessment was not clarified. This resulted in a follow-up being done with some of the participants within the risk management unit. These participants were followed up as they were involved in the IT risk assessment process. This question was important as it impacted the development of the risk management framework.

4.3.6 Present and discuss the results

The key themes were identified as they had a link with the data collected with a potential to address the research questions that the study intended to address, as illustrated in Table 4.12.

Table 4.12: Summary of the emerged themes

THEME NO.	THEME	SUB-THEME
1.	**Access to ICT tools and resources**	1.1 ICT Tools and resources availability
		1.2 Access and use of ICT resources
2.	**Usefulness of the ICT resource**	2.1 Frequency of using the resource and ICT skills
3.	**Impact of ICT**	3.1 Value of ICT resources

The main themes for the survey as illustrated in Table 4.12 were: 1) Access to ICT tools and resources, 2) Usefulness of the ICT resource, and 3) Impact of ICT. Each of these themes is derived from the literature presented in Chapter 2. Furthermore, various sub-themes emerged during the analysis of data that were linked to the main themes. The sub-themes emerged through the manual analysis and coding of the entire data set. This allowed the identification of all trends and the consistency of these patterns. This was made possible through writing notes on patterns that reinforced the use of ICT in risk management, and these notes were maintained throughout the analysis.

The next section discusses each theme outlined in Table 4.12 for the qualitative survey.

4.3.6.1 Theme 1: Access to ICT tools and resources

Research question answered - *Sub-question 1: What ICT tools are available to support the implementation of risk management activities?*

Access to ICT tools and resources informs the theme one of this study's major findings and is derived from the first sub-objective – to understand the technological tools utilised to implement risk management. In this study, ICT tools are referred to as the devices while resources are identified as applications and software packages. To investigate the extent to which ICTs are used to implement risk management processes in the public sector, the following questions were probed to receive the response that informed this theme (Annexure F; Annexure G):

Section two of the questionnaire sought to determine the access and use of ICT in risk management. Question 2.1 A was: "*Do you have the following ICT equipment? Please select the ones you currently have*". In this instance, the equipment forms part of the tools. The participants indicated that they had access to most of the ICT equipment. The availability of ICT tools and resources was confirmed through Question 2 of the interview questions.

Question 2.1 B *"Do you have access to the following? Please select the ones you currently have"* sought to determine the access to ICT resources. After determining the role that each participant played in risk management during the interviews, Question 2 "Do you have access to any ICT tools e.g. computer, system, internet, etc.?" of the interviews was asked and it confirmed the findings from the questionnaire. Furthermore, to determine the purpose of each of the tools and resources made available, Question 2.2C of the questionnaire was "*What do you use the following resources for (indicate for what purpose do use the IT resource for)?".* To validate this information, Question 3 of the interview asked*, "How do you use ICT tools in your daily risk management activities?"*

The detailed findings relating to this theme are presented and discussed under the following sub-themes:

4.3.6.1.1 Sub-theme 1.1: ICT Tools and resources availability

This sub-theme seeks to understand the availability and accessibility of ICT tools and resources. The participants listed many tools and resources which included laptops and or desktops, Microsoft Office package, Microsoft Teams, SAP GRC system, network drive, and smartphones that were made available to them as illustrated in Figure 4.4.

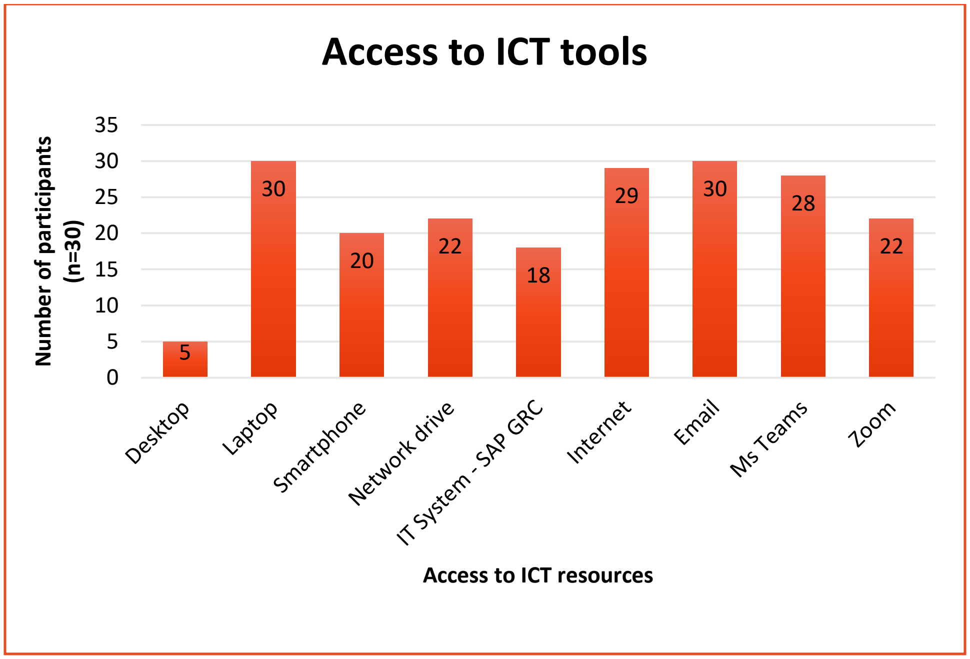


Figure 4.4: Access to ICT tools and resources

As illustrated in Figure 4.4, all the participants indicated that they had laptops and email. Among these participants, five also had desktop computers. With these ICT tools, 22 participants are connected to the network drive which is a storage facility for risk-related documents. For the network drive to be connected, the laptops or desktops need an Internet connection which has been made available to 29 participants. Twenty participants had smartphones. The smartphones had a WhatsApp facility that was used for communicating with various stakeholders. Communication groups are created on the

WhatsApp facility for awareness and communicating risk-related information including emerging risks.

The officials were further provided with Microsoft Teams for virtual meeting purposes and the sharing of files. Twenty-eight participants responded that they had access to Microsoft Teams while twenty-two of them had Zoom. Although these participants both had Microsoft Teams and Zoom, Microsoft Teams was a preferred meeting virtual platform for the department. Eighteen participants indicated that they had the SAP GRC system installed on their machines. The system is used to identify and manage departmental strategic and operational risks. Only sixty percent (60%) of the participants indicated they had the SAP GRC system installed in their machines.

Based on the preceding discussion, the officials have been allocated reasonable ICT tools to support and enable their daily risk management activities.

4.3.6.1.2 Sub-theme 1.2: Access and use of ICT resources

This sub-theme intends to respond to the first objective as presented in Section 1.4.1 to investigate the extent to which ICTs are used to implement risk management processes in the public sector. While the resources are made available to the officials, it does not guarantee the access and utilisation of the ICT resources. Once the ICT resources are made available, access should be granted to the users. This is the first step towards determining whether the officials embrace the availability and access to ICT. The resources that were made available with the laptops or desktops included Microsoft packages – Word, Excel, Outlook, and PowerPoint.

The next question was to understand for what purpose the participants used each of the ICT resources made available to them. The question was 2.2 C: "*What do you use the following resources for (indicate for what purpose do use the IT resource for)?".* This question was confirmed during interviews by Question 3. The participants specified the following resources while indicating how they were using them as presented below.

The first IT resource highlighted was the SAP GRC system. This system is used together with Microsoft Excel and Internet Explorer. The system's users required internet access for its use. The system was used to conduct risk assessments, update the risk registers, monitor the risks, and generate reports. During the fiscal year, the risk assessments were conducted using face-to-face workshops. The outcomes of the risk assessment were documented on the Excel risk register template. The risk registers were communicated through Microsoft Outlook (email) with various risk owners and other stakeholders for implementation and reporting. The risk champions were expected to update their risk registers on the system. The updated risk registers were managed and monitored on the system quarterly. The SAP GRC system allows the risk owners, risk practitioners, risk champions, and other officials who have access to the system to generate various management reports. In addition, the internet was used to conduct risk-related research.

The other resource identified as critical was PowerPoint. PowerPoint was used together with Microsoft Teams. This resource was used to do presentations for the risk forums and awareness throughout the department. Microsoft Teams provided a virtual connection platform for various meetings such as risk assessments and stakeholder engagements. After the risk assessments were conducted through Microsoft Teams or face-to-face meetings, the risk register on the SAP GRC system was updated. Apart from the system, the risk management reports were prepared using Microsoft Word. These reports were presented to various governance structures like risk management and audit committee using PowerPoint. Microsoft Word was also utilised for various correspondence, submissions, memos and to develop risk management documents. These documents were sent to various stakeholders using Microsoft Outlook (email). Some of the participants gave a general statement that they were using the ICT resources to perform their daily activities while others did not highlight all the resources. The interviews gave a clear understanding of how all the resources were utilised, which confirmed the findings of the survey.

To determine whether the participants were using all the ICT resources made available to them**,** Question 2.2 D *Why are you not using the ICT resources provided (please indicate the reason next to the resource)?* was asked. All the participants indicated that they were using all the resources in cases where there were no challenges like data or internet connection.

The findings for theme two determined how useful the resources were to support risk management.

4.3.6.2 Theme 2: Usefulness of the ICT resource

Research question answered - *SQ 2: How will using ICT contribute towards the effectiveness of the risk management function within the organisation?*

This theme seeks to determine whether the participants valued having access to ICT resources. This may be demonstrated by how the participants welcomed innovation. This theme is derived from the first sub-objective to understand the technological tools utilised to implement risk management.

To understand how the participants were using the ICT tools made available to them, the following questions were asked: *Question 2.2 A How often do you use the following resources?* The participants had a choice between daily, weekly, monthly, and quarterly as illustrated in Table 4.13. In response to Question 3 of the interviews, the participants provided in-depth information on their use. Furthermore, Question 2.2 B was asked to determine the competency of the participant on the resources illustrated in Table 4.13.

Table 4.13 illustrates the ICT resources that the participants had access to, how often they utilise each of these resources, and lastly, the level of self-assessed competency for the resource. The percentage for the competency has been rounded off to the nearest value. Sub-theme 2.1 discusses the findings demonstrated in Table 4.13. In addition, the views of the participants on the usefulness of the individual ICT resource will be discussed.

Table 4.13: Skill competency against ICT

ICT RESOURCE	FREQUENCY OF USE	COMPETENCY - PERCENTAGES
Network drive	Daily – 100%	Expert – 0% Advanced - 37% Proficient - 40% Basic - 17% Limited - 6%
IT System (SAP GRC)	Daily – 20% Weekly – 13% Monthly - 20% Quarterly - 47%	Expert - 10% Advanced – 0% Proficient – 43% Basic- 23% Limited - 17% Unknown - 7%
Internet Explorer	Daily – 100%	Expert – 6%, Advanced - 57% Proficient - 33% Basic - 3% Limited - 7%
Microsoft Teams	Daily - 33% Weekly - 47% Monthly - 17% Quarterly - 3%	Expert – 0% Advanced – 20% Proficient – 50% Basic – 27 Limited - 3%
Microsoft Powerpoint	Daily - 20% Weekly - 23% Monthly - 40% Quarterly - 17%	Expert - 3% Advanced - 40% Proficient - 47% Basic - 10% Limited - 0%

4.3.6.2.1 Sub-theme 2.1: Skill competency

For the list of the ICT resources illustrated in sub-theme 1.1, the participants indicated their frequency of using these resources together with the level of the skill they possess for each resource as follows:

i) Network drive (ND)

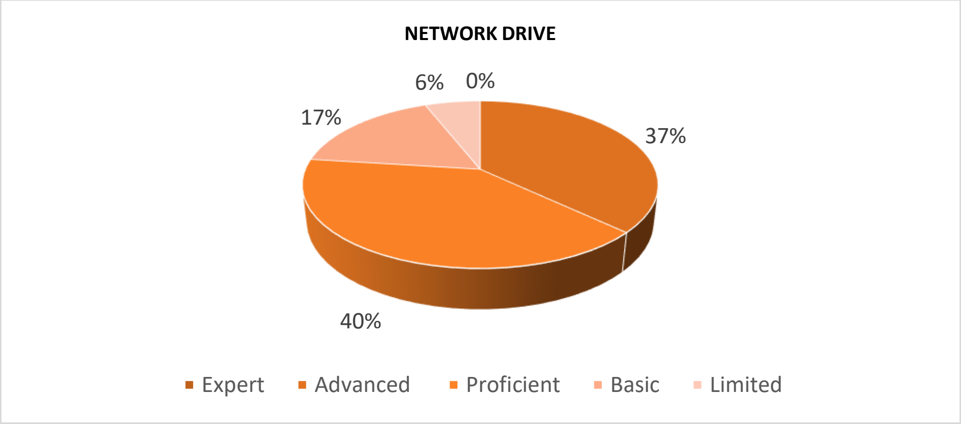


Figure 4.5: Self assessed competency level for ND

The competency for the ND is illustrated in Figure 4.5. While the participants upload documents on the network drive, the participants administer the drive for their business units which requires them to at least have technical abilities. Thirty-seven percent (37%) of the participants indicated that their competency level was advanced, 40% was proficient, 17% was basic, and six percent (6%) were limited. The risk practitioners and the appointed risk champions were granted access to the drive through the local network connected to the departmental server. The network drive was utilised daily by all the participants. The risk management team engages and supports all the branches, provincial and cluster offices. Risk management-related documents were shared with the stakeholders in these business units. The network drive provided a central point where documents are placed to document management. These documents included the risk management framework, policies, and strategies. Furthermore, this network drive was used to upload and manage the portfolios of evidence submitted quarterly to support implemented risk mitigations. The users were confronted with the risk of loss of information while utilising the network drive. To mitigate these information security risks, the risk champions were granted access upon approval by the risk management team. In addition, the risk champions were provided the read-only rights on the main folder for risk management as a risk mitigating factor. This meant they were unable to delete any other information. However, the risk champions were granted full permission to their respective folders where they updated their submissions. The participants found access to the network drives to be useful. The network drive depended on the network availability, which participants already indicated was unreliable. The participants indicated that they could not access the drive during the lockdown, irrespective of having a virtual private network (VPN). The inability to access the network drive resulted in the users not being able to upload and retrieve information to assist them with future risk assessments. The VPN had become increasingly important during the COVID-19 pandemic for public sector institutions. An increasing number of officials required the connection through the VPN while working from home. This may have added more pressure to the department as the demand for this network increased.

The next resource discussed is SAP Governance Risk and Compliance (GRC) system.

ii) SAP GRC

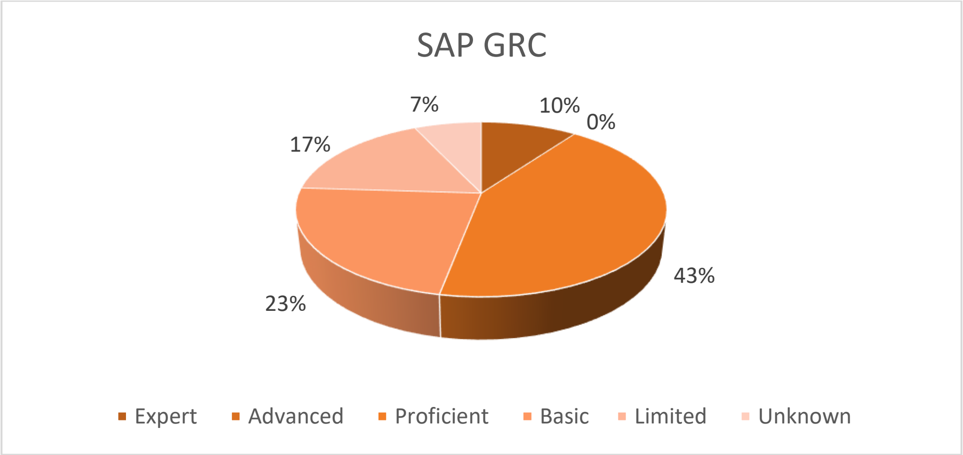


Figure 4.6: Self-assessed competency level for the SAP GRC

The competency for the SAP GRC is illustrated in Figure 4.6. Ten percent of the participants indicated that their competency level was expert, 43% was proficient, 7% was advanced, 23% was basic, and 17% was limited. Seven percent (7%) of the participants did not indicate their level of competency.

Twenty percent (20%) of the participants used the system daily. This percentage was made up of all the five risk practitioners who drive the implementation of risk management and one IT official who provides support to the rollout of the system. The risk practitioners further ensured that the risk champions are trained so that they can be granted access to the system. Furthermore, 13% were using the system weekly, 20% monthly, and 47% quarterly.

This revealed that most participants only used the system quarterly although the risk management team preferred that the users utilised the system often for better management of risks. Risk management reports to various governance structures quarterly. Using the system quarterly could mean these users only used it during reporting periods. These are concerning findings as it may be difficult to determine the system's efficiency and effectiveness.

The participants perceived the SAP GRC system to have the potential to improve the risk management process, yet the participants highlighted numerous challenges that resulted in the system not being fully utilised. RP_C argued that the system has the potential to bring efficiency to risk management operations. Likewise, RP_E emphasised that the system allows users to conduct risk assessments remotely, which was beneficial during the lockdown period. The benefits highlighted included an automated risk assessment tool where risk-related data collection and analysis is automated, ease of reporting, and the ability to update registers while keeping an audit trail. RC_F suggested that automating the risk management system fully could bring effectiveness and efficiency to the risk management process, yet RC-F further pointed out that this depends on the full functionality of the system.

The system's ineffectiveness was identified so the organisation can enhance it for better functioning. These included the system being slow while processing the captured information, challenges with the server affecting the system capability, network connection challenges, shortage of skilled resources, capacity, and insufficient training. Nine participants from the survey emphasised the network connectivity challenges that impact the system functionality. This was supported by five participants from the interviews. Some examples of what the participants said include:

Survey	**Interview**
RP_03 *"…unreliable network…"*	**RC_H** *"…network connection for SAP during lockdown".*
RC_08 "…*lack of network access…"*	**RP_C** *"And the other challenge that is beyond is the network, while we are busy on the system…sometimes we get network challenges".*

To alleviate the system downside, RC_D suggested that for the organisation to effectively utilise ICT, the department needs to invest in IT infrastructure. If the organisation maintains the IT infrastructure, risk management may be improved with the adoption of ICT. Interestingly, PWC (2015) emphasises that the organisations that invest in GRC tools report that the effectiveness of their ERM programmes has realised efficiency and transparency in line with their risk information. This supports the views of the participants who believe that, if the department is not investing in its IT, it will not fully enjoy the benefits.

The next resource discussed is internet explorer.

iii) Internet Explorer (IE)

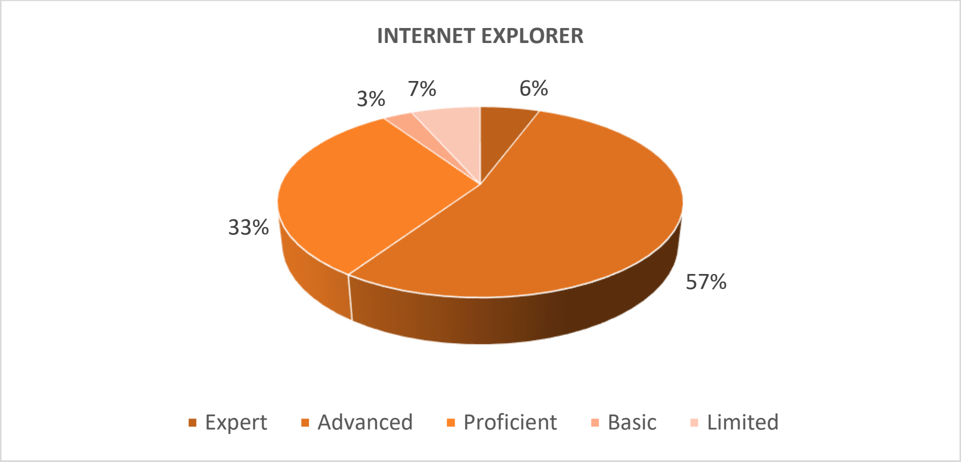


Figure 4.7: Self-assessed competency level for the IE

The competence of the IE is illustrated in Figure 4.7. Six percent (6%) of the participants indicated that their competency level was expert, 57% was advanced, 33% was proficient, 3% was basic, and 7% was limited. The participants used internet explorer as an enabler for risk-related research purposes and an enabler to the risk management responsibilities. This required a technical ability to reduce the potential loss of information. The use of internet explorer was influenced by the network connection. The participants raised concerns about network connection, which affects daily risk management operations. Further, the participants were granted a virtual private network connection during the lockdown period which ensured continuity in their activities that required IE. IE was used daily for research and other resource connections. The next resource discussed is Microsoft Teams.

iv) Microsoft Teams (Ms Team)

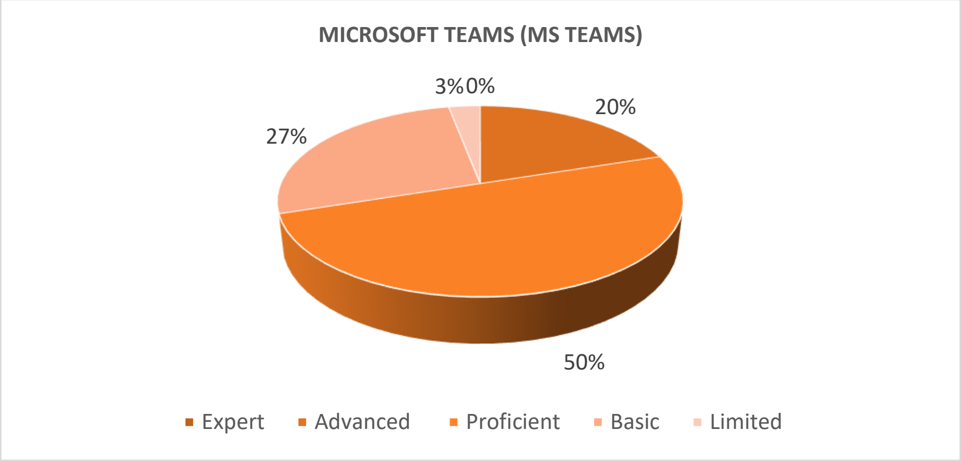


Figure 4.8: Self-assessed competency level for the Ms Teams

The competence of Ms Teams is illustrated in Figure 4.8. Twenty-three percent of the participants indicated that their competency level was advanced, fifty percent was proficient, and twenty-seven percent was basic. Out of the thirty participants, thirty-three percent (33%) were using Ms. Teams daily, forty-seven percent (47%) weekly, seventeen percent (17%) monthly, and three percent (3%) quarterly. The participants who were using MT daily include three IT officials. These are some of the views that the participants had in line with the use of Microsoft Teams:

- RC_E reported that MS Teams was used daily, especially with the COVID-19 pandemic where meetings were held virtually.
- RC_G further indicated that during the COVID-19 pandemic, the risk assessments were conducted on MS Teams together with other engagements.

The participants indicated that Microsoft Teams provided convenience to the department during the lockdown period. This is the period when the country was affected by the COVID-19 pandemic that forced government departments to close doors in compliance with the lockdown regulations. While the officials in the department were required to work from home, most of the officials managed to continue with their daily operations using Microsoft Teams. The participants indicated that they relied mostly on Microsoft Teams to conduct the risk assessments, risk awareness sessions, and arrange the risk management committee meetings and other engagements with stakeholders across the department. Microsoft PowerPoint was useful when they needed to present to various stakeholders on this platform.

These findings show that MS Teams fully supported the risk management activities during the lockdown period. Most participants confirmed the usefulness of Microsoft Teams, especially during the lockdown period owing to the COVID-19 pandemic. The next resource discussed is Microsoft PowerPoint.

v) Microsoft PowerPoint (PPT)

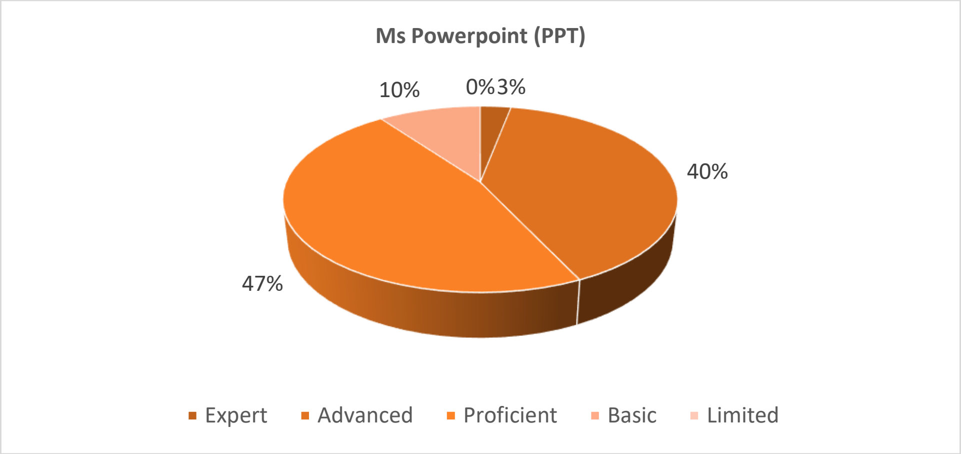


Figure 4.9: Self-assessed competency level for the PPT

The competency for PPT is illustrated in Figure 4.9. Three percent (3%) of the participants indicated that their competency level was expert, forty percent (40%) was advanced, forty-seven percent (47%) was proficient, and ten percent (10%) was basic. The risk management team provided reports to various governance structures that includes top management, risk, and audit committees. This unit further conducted awareness to create and strengthen the culture of risk management within the department. The PPT together with Microsoft Teams was used to support these activities. Twenty percent (20%) of participants used PPT daily, twenty-three percent (23%) weekly, forty percent (40%) monthly, and seventeen (17%) quarterly.

There were additional resources not rated for competency. These resources emerged from the survey indicating the frequency of use, as indicated in Table 4.14.

Table 4.14: Frequency of use

Frequency of use	Percentage of participants using Microsoft Word	Percentage of participants using Microsoft Excel
Daily	97%	60%
Weekly	3%	23%
Monthly	-	7%
Quarterly	-	10%

vi) Microsoft Word

As displayed in Table 4.14, 97% of participants indicated that they were using Microsoft Word daily while only 3% indicated they used it monthly. Microsoft Word was mostly used for developing the framework and policy documents for risk management, submissions to request approval of various risk management documents, and reporting to various governance structures. Most of these activities were performed daily and informed by the reporting structures' timeframes.

vii) Microsoft Excel

As displayed in Table 4.14, the survey reveals 60% of participants, which includes that the risk management team and risk champions were utilising Excel daily, 23% weekly, 7% monthly, and 10% quarterly (IT officials).

Theme 1 indicated that a risk register was developed using an Excel template. This template allowed users to manage and monitor the risk register quarterly. This template was automated to allow risk calculations before the department procured the SAP GRC.

The risk champions were expected to continuously update this template with emerging risks, an update on the implementation of the mitigations, and any other changes on the risks with the support of the risk practitioners. Most of the risk champions found the template to be more useful. The risk champions thought the Excel spreadsheet template was easy to use compared to the system, yet, while the risk practitioners agreed with the user-friendliness of the template, they highlighted challenges in this template which resulted in the procurement of the IT system. The challenges included that the template was easily manipulated and corrupted from one user to the other. The department is currently moving towards the utilisation of the IT system. These were some of the views of the participants that were interviewed:

RP_C argues that

> *"the system should be fully utilised to conduct risk assessments as it has the capability instead of duplicating efforts between the manual process and the system".*

On the other hand, RC_G acknowledges the need to move to the system. However, RC_G stated that amid the ICT challenges they are facing, the Excel template becomes a safety net. This highlighted that, while it would be better to automate, the organisation should not overlook that Excel can be a backup in cases where there are challenges. While the department intended to move towards using the IT system, the users were comfortable with using Excel based on the responses above. The participants who were within risk management strongly raised the need to move towards an IT system. One of the participants identified resistance to change as one of the factors that most people preferred the Excel template and not utilising the IT system. This is how one participant viewed the issue of reluctance to change:

> *"I think change management is a problem because you will get officials who have been in the department for very long and even with age. As we know ICT comes with changes more often, so you will get them sticking to the old ways and not want to adjust to the new changes that are happening in the ICT environment" – RP_C.*

This was an indicator that the risk management team should take cognisance of the differences among the risk champions to ensure that training is tailor-made to accommodate their needs. The next section discusses theme 3 as presented in Table 4.4 to determine if the integration of ICT in all risk management activities improves the effectiveness of risk management.

Overall, Question 2.2E *Do you see having access to ICT resources important?* was asked to determine the importance of having access to ICT resources. Twenty-nine participants strongly agreed while one participant agreed that having access to ICT resources was important.

Lastly, Question 2.2F *Do you see using ICT resources in risk management useful?* was asked to understand the usefulness of the ICT resource in risk management. Table 4.15 illustrates the responses received on the importance and usefulness of the available ICT resources.

Table 4.15: Importance and usefulness of ICT resource

Response	Number of participants who see having access to ICT resources important?	Number of participants who see using ICT resources in risk management useful?
Strongly agree	30	24 (80%)
Agree	0	5 (17%)
Do not know	0	1 (3%)

All 30 participants regarded having access to the ICT resources as important for them to perform their daily tasks. Eighty percent (80%) of these participants strongly agreed that it is useful to utilise these resources to implement their daily risk management activities. In addition to that, 17% agreed on the usefulness of these resources while only 3% did not know. Considering the number of participants who either strongly agree or agree, it is safe to conclude that ICT has been found useful in implementing risk management.

4.3.6.3 Theme 3: Impact of ICT

Research question answered: *SQ 3: What techniques are currently being used to conduct technology-related risk assessments?*

This theme sought to determine the contribution of ICT to the implementation of risk management activities in the department. This theme derives from the second sub-objective – to determine if the integration of ICT in all risk management activities improves the effectiveness of risk management. This objective intends to respond to sub-question 2 – how will using ICT contribute towards the effectiveness of the risk management function within the organisation? Furthermore, this theme derives from the third sub-objective – to investigate the methodologies used to conduct ICT risk assessment in the organisation. This objective intends to respond to sub-question 3 – what techniques are currently being used to conduct technology-related risk assessments? To determine the impact of ICT to risk management, Question 3.1 of the questionnaire required the participants to rate the provided statements about using technology in implementing risk management activities.

The next section presents sub-theme 3.1 considering the value of ICT on the activities illustrated in Question 3.1 of the questionnaire.

4.3.6.3.1 Sub-theme 3.1: Value of ICT resources

This sub-theme reviewed the impact of ICT tools on each of the risk management (RM) process activities. The risk management process that the public sector adopted is illustrated in Figure 4.10. Section 3 of the questionnaire collected data to understand the impact of using ICT to implement risk management. Eight statements were tested against the impact of using technology using the Likert scale - Strongly Agree (SA), Agree (A), Don’t know (DK), Disagree (D), and Strongly disagree (SD). To understand the importance and dominance of these statements, numbers were utilised for analysis purposes. The results are presented in Table 4.16.

Table 4.16: The impact of ICT in RM

LIKERT SCALE STATEMENT	RESPONSES
1.Identify and assess risks accurately	
Strongly agree	17 (57%)
Agree	13 (43%)
Don’t know	-
Disagree	-
Strongly disagree	-
2.Communicate risk activities efficiently	
Strongly agree	17 (57%)
Agree	12 (40%)
Don’t know	1 (3%)
Disagree	-
Strongly disagree	-
3. Ability to define risk appetite levels	
Strongly agree	12 (40%)
Agree	17 (57%)
Don’t know	1 (3%)
Disagree	-
Strongly disagree	-
4. Allows easy submission of the portfolio of evidence	
Strongly agree	18 (60%)
Agree	11 (37%)
Don’t know	1 (3%)
Disagree	-
Strongly disagree	-
5. Effective capturing of quarterly progress against mitigations	
Strongly agree	14 (47%)
Agree	15 (50%)
Don’t know	1 (3%)
Disagree	-
Strongly disagree	-
6. To manage and monitor identified risks better	
Strongly agree	17 (57%)
Agree	13 (43%)
Don’t know	-
Disagree	-
Strongly disagree	-
7. Assign responsibility and accountability to relevant managers accurately	
Strongly agree	17 (57%)
Agree	13 (43%)
Don’t know	-
Disagree	-
Strongly disagree	-
8. Improve reporting of risks	
Strongly agree	16 (53%)
Agree	12 (40%)
Don’t know	2 (7%)
Disagree	-
Strongly disagree	-
9. Allows to propose emerging risks in a timely manner	
Strongly agree	16 (53%)
Agree	13 (43%)
Don’t know	1 (3%)
Disagree	-
Strongly disagree	-

In determining the impact that the ICT has on risk management, the analysis of this impact was measured against the risk management process where each activity is relevant to a step in the risk management process illustrated in Figure 4.10, shown by the numbers from 1 to 7. To follow through this sub-theme, Figure 4.10 needs to be read together with Table 4.16 to understand where each activity fits into the process and how ICT contributes towards risk management through these activities.

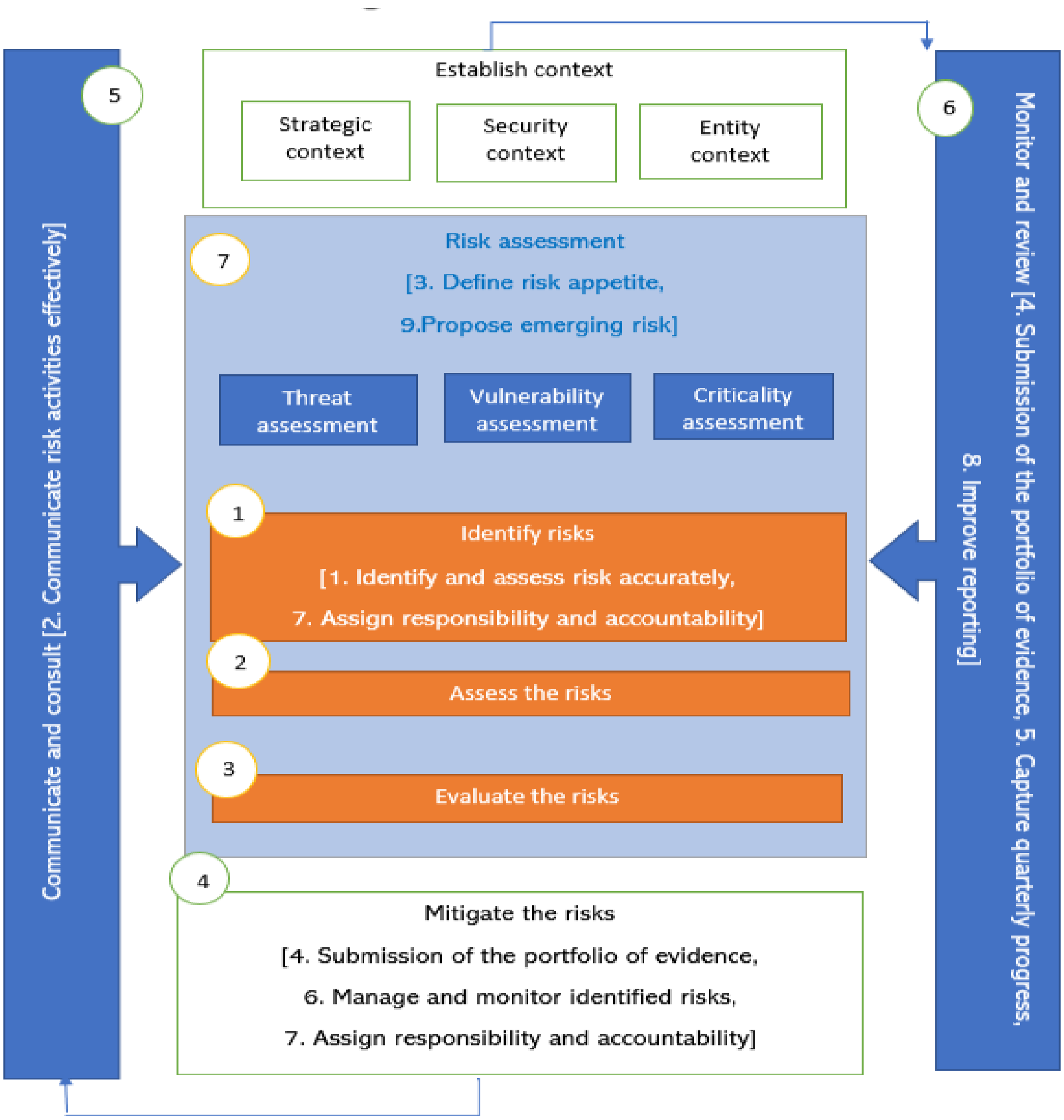

Establish context
Strategic context
Security context
Entity context
5
6
7
Risk assessment
[3. Define risk appetite,
9.Propose emerging risk]
Threat assessment
Vulnerability assessment
Criticality assessment
1
Identify risks
[1. Identify and assess risk accurately,
7. Assign responsibility and accountability]
2
Assess the risks
3
Evaluate the risks
4
Mitigate the risks
[4. Submission of the portfolio of evidence,
6. Manage and monitor identified risks,
7. Assign responsibility and accountability]
Communicate and consult [2. Communicate risk activities effectively]
Monitor and review [4. Submission of the portfolio of evidence, 5. Capture quarterly progress,
8. Improve reporting]

Figure 4.10: Risk assessment process

Source: Alijoyo and Norimarna (2021)

Before the identification of risks, the risk management process requires the establishment of the context in which risks will be assessed. Following that, a risk identification commences as illustrated in Figure 4.10. Risk identification (1) is the process where the risk owners identify possible risks aligned with their business objectives. Once a risk is identified, risk assessment (2) follows where the risk owners analyse all the attributes that trigger the risk. Following the understanding of these attributes, the risk owners evaluate

(3) the risk to determine its level, indicating whether it needs to be mitigated (4) or not. This process is called the risk assessment (7). Risk mitigation is an action measure aimed at reducing the risk severity. The risk is later communicated (5) to the relevant risk owners and other governance structures for monitoring (6). The key activities for risk assessment and management in the organisation are mapped within Figure 4.10 and are discussed as follows:

i) Identification and assessment process

The risk identification and assessment process is a structured process of identifying the key risks that the organisation is exposed to, these risks are analysed and assessed to understand the level of exposure (Srinivas, 2019). The SAP GRC system that emerged as a technology tool that supports risk management in the findings has the functionality to identify the risk. The automation of the risk assessment provides efficiency in the process. This activity is illustrated as (7) in Figure 4.10. The risk assessment results in the expression of the potential loss that an organisation may incur while delivering on the specific objective. This process results in the development of a risk register. In cases where the risk attributes such as impact, likelihood, and severity change in the risk register, the user easily updates the system.

An understanding of the risk exposure informs the allocation of resources to mitigate these risks. This process was facilitated by the risk practitioners with the assistance of the risk champions. However, the risk owners identify and assess the risks in their respective areas of responsibility. To ensure the adequate monitoring of the risk, a risk owner is assigned responsibility and accountability for each risk manually and on the system as illustrated in Figure 4.10 (1 and 6). Srinivas (2019) identified factors affecting the analysis of risk such as cost and resources required. The results indicated that 57% of the participants strongly agree while 43% agree that ICT has a positive contribution in identifying and assessing risks within the organisation.

ii) Communication of risk

George (2020) argues that having a risk register assists the organisation in communicating the risks across the organisation for monitoring. The organisation developed the risk registers for various business units and captured them on the system to allow better communication with multiple risk owners. A simple example is that of the project risk registers where risk owners reside in different areas that deal with construction, project management, and engineering. This activity allowed the allocation of three risk owners respectively, as illustrated in Figure 4.10 (5). The participants acknowledged the importance of communicating risk information and further indicated that ICT plays a critical role in this process. The organisation implements SAP GRC, which had the function to communicate the risk information to the various risk owners at once. The respective risk owners received notifications in their email inboxes to notify them of the actions required from them. The participants further indicated that the department used various ICT tools that include Microsoft Teams, PowerPoint, and videos to communicate risk-related information to the stakeholders. Out of the total number of participants, 57% strongly agree, and 40% agree that ICT is useful to ensure effective communication of risks while only 3% disagree. The participants who disagreed may be influenced by the concerns that the SAP GRC system was still new and not being fully utilised.

One participant, RP_A, stated that while the system was playing a crucial role in supporting risk management, the users need to be confident to use the system before discontinuing the manual system. The effectiveness of risk communication on the SAP GRC may be influenced by the organisation being reluctant to change. One participant, RC_F, advised that the risk champions were from various age groups. The officials who had been in the department long within the oldest age group were not willing to use the system. The issue of computer literacy had been identified as one of many reasons for this reluctance. Some participants, such as RC_D, observed that the challenge could be the skill of utilising the system.

iii) Definition of risk appetite levels

For adapting innovative technologies in risk management, data risks should be considered as a basis to risk categorisation linked to the specific risk appetite statement (Zainudin et al, 2019). The organisation needs data to gain insights into the impacts of strategic and operational decisions they make (Martens & Rittenberg, 2020). Martens and Rittenberg (2020) further argue that risk appetite needs to be linked with the organisation’s strategy and plans to avoid conflicts. This activity allowed the determination and assigning of risk appetite and tolerance levels to individual risks. The SAP GRC system had already been configured to support this process. This is an activity in the risk assessment process (7) in Figure 4.10. Forty percent (40%) of participants strongly agree while 57% agree that ICT was useful in defining the levels of risk appetite, while 3% did not know. The organisation was only starting the rollout of the risk appetite and tolerance framework using videos to create awareness through Microsoft Teams. While technology has a potential to accelerate the determination and alignment of risk appetite, this process fully depends on the commitment of management as the decision makers.

iv) Submission of the portfolio of evidence

This activity allowed the submission of the portfolio of evidence (PoE) for the implemented mitigations. The submission of the PoEs in Figure 4.10 (4 and 6) is done quarterly for accurate reporting. The risk owners are required to support the progress made in implementing the risk mitigations with the PoEs. The organisation relied on the network drive and the SAP GRC system for managing the evidence portfolio. It is important to note that 73% of the participants had access to and utilised the network drive while 60% had access to the SAP GRC. Furthermore, the availability and access to the network drive allowed the risk champions and practitioners to safely store, process and manage data related to the implemented mitigations. The IT department grants access to the network drive to the users on request from the risk management team for security purposes. Only one risk champion from the respective business unit is granted access with permission to add and remove data in specific folders. However, the SAP GRC system had the functionality to submit and monitor the portfolio of evidence submitted. The system had an audit trail to determine who has removed or added documents for security purposes.

Sixty percent (60%) of the participants strongly agree while 37% of the participants agree that ICT plays an effective role in providing a portfolio of evidence. Only 3% do not know whether ICT supports the submission of the PoEs.

v) Capturing the quarterly progress

As the reporting is done quarterly, the system gets updated with the quarterly progress. This activity is done as illustrated in Figure 4.10 (6). The system can track the progress made on the implemented mitigations. This progress is supported by activity four where PoEs are submitted to support the quarterly progress. Forty-seven percent (47%) of the participants strongly agree while 50% agree that ICT has a positive impact on the capturing of the reports. Lastly, only 3% do not know whether ICT plays a role in this activity.

vi) Manage and monitor identified risks

This activity is closely related to the capturing of the quarterly progress of mitigations and the submission of the portfolio of evidence (PoE) (activities 4 and 6). This is where monitoring the management of risks is done to determine whether the risks are managed effectively or not. The system provides various management reports that can be customised for various purposes. Fifty-seven percent (57%) of the participants strongly agree while 43% agree that ICT has an impact on this activity.

vii) Assigning responsibility and accountability

The responsibility to ensure that risks are effectively managed resides with management (George, 2020; Srinivas, 2019). On the other hand, Zainudin et al., (2019) identify risk ownership as one of the key aspects to support the implementation of risk management. This activity (Figure 4.10,1 and 4) allowed for the assignment of responsibilities to various risk owners, as discussed in activity two – communication of risk. The concern is that most of the risk owners did not have access to the system, which resulted in the benefit of the system not being realised. Fifty-seven percent (57%) of participants strongly agree while 43% agree that ICT is useful in assigning responsibility and accountability of risks to relevant risk owners.

viii) Improves reporting

This activity is supported by activities 4 (allows easy submission of PoEs), 5 (capturing of quarterly progress), and 6 (managing and monitoring identified risks). The success of these activities leads to improved reporting. Fifty-three percent (53%) of participants strongly agree while 40% agree that ICT plays an effective role in an improved reporting process to various governance structures. Lastly, 7% of the participants did not know if ICT plays a role in improving reporting.

ix) Proposition of emerging risks

This activity allowed the risk champions and the risk owners to propose the emerging risks as shown in Figure 4.10. As illustrated in Figure 4.10 (7), the risk proposal is done during the risk assessment process. An emerging risk is defined as a new risk that has the potential to materialise (Brocal et al., 2019). Furthermore, the emerging risk can be triggered by technological innovations and or unfamiliar conditions (Brocal et al., 2019). The department had a process of identifying and managing emerging risks and follows a formal process to gather relevant data for them to be managed effectively. The SAP GRC system allowed the proposal of the emerging risks to the risk management team for approval based on relevancy. The risk management team is granted access to the system as super users. The super users have full access to the system. The risk management team receives the notification through email notification to either approve or reject the risk. Furthermore, the approval or rejection of a risk requires an analysis as indicated in Activity 5. If the analysis meets the criteria as a risk, the super user approves the risk for further assessment. Fifty-three percent (53%) of the participants strongly agree while 43% agree that ICT plays a role in proposing an emerging risk. Only 1% did not know whether ICT has a positive role in emerging risks.

The analysis of each of these activities suggests that the ICT, specifically the SAP GRC system, has the capability of improving the risk management process by providing automation to all the risk management processes.

To further validate the survey findings, an interview question was asked to support the survey's findings. Some of the responses from the participants for Question 4 *Is ICT playing an effective role in implementing risk management activities?* are presented in the extract next.

Participant	Response
RP_B	*“Yes, the reason I am saying yes is that it makes things easy. We can connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties”.*
RC_J	*“Yes, risk management integrates with various business processes in the organisation. ICT plays a role where we can integrate reporting”.*

Out of the ten participants who responded to the question, only one official indicated that ICT is not playing an effective role in risk management owing to the organisation not financially investing in ICT. An important aspect is that the participant is in the eldest age category that ranges between 47 and 60, as illustrated in Section 4.2.2. It has been found that the participants in this category are reluctant to adapt to technology. However, RP_B (the risk practitioner) believes that ICT plays a fundamental role to support risk management activities. RC_J (the risk champion) supported this view stating that the organisation can benefit from integrating ICT into the business processes to support improved reporting.

It is interesting to see that not only the risk management team realises the contribution of ICT in the risk management process. It should also be noted that some of the participants acknowledge that IT plays a role in risk management although they did not specifically refer to it as effective (RP_A said: “I would not say effective, but ICT is playing a role”). The results on this sub-theme indicated that the participants believe that the use of ICT contributes positively to risk management activities. The participants were clear on the technology tools utilised for risk assessment in the organisation. Section 4.2.4 discusses the challenges that the participants identified as hampering the integration of ICT in risk management. The corrective measures to address these challenges are also presented in this section.

4.3.7 Challenges identified by the participants

The last section of the questionnaire determined the challenges affecting the participants while utilising ICT in risk management and the workable solutions proposed by the participant. The first question: Question 4.1 *In your own view, what are the challenges affecting the use of ICT in risk management within the department?* exhausted the detrimental factors that result in the participants being unable to fully utilise the technology when implementing risk management. The participants mentioned various challenges and corrective measures as illustrated in Figure 4.11.

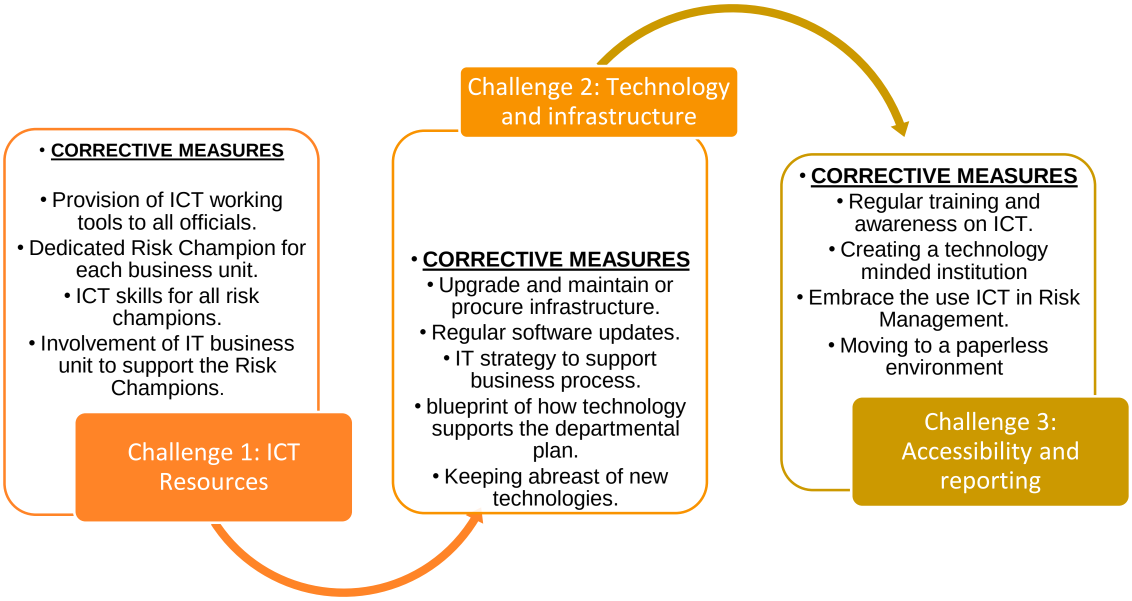

• CORRECTIVE MEASURES
• Provision of ICT working tools to all officials.
• Dedicated Risk Champion for each business unit.
• ICT skills for all risk champions.
• Involvement of IT business unit to support the Risk Champions.
Challenge 1: ICT Resources
Challenge 2: Technology and infrastructure
• CORRECTIVE MEASURES
• Upgrade and maintain or procure infrastructure.
• Regular software updates.
• IT strategy to support business process.
• blueprint of how technology supports the departmental plan.
• Keeping abreast of new technologies.
• CORRECTIVE MEASURES
• Regular training and awareness on ICT.
• Creating a technology minded institution
• Embrace the use ICT in Risk Management.
• Moving to a paperless environment
Challenge 3: Accessibility and reporting

Figure 4.11: ICT corrective measures

While the study intended to determine the contribution of ICT in supporting risk management, it was critical to understand the factors affecting the adoption of ICT in risk management. These challenges also influenced technology-related risk assessments. The next section discusses the challenges as follows:

4.3.7.1 Challenge 1: ICT resources

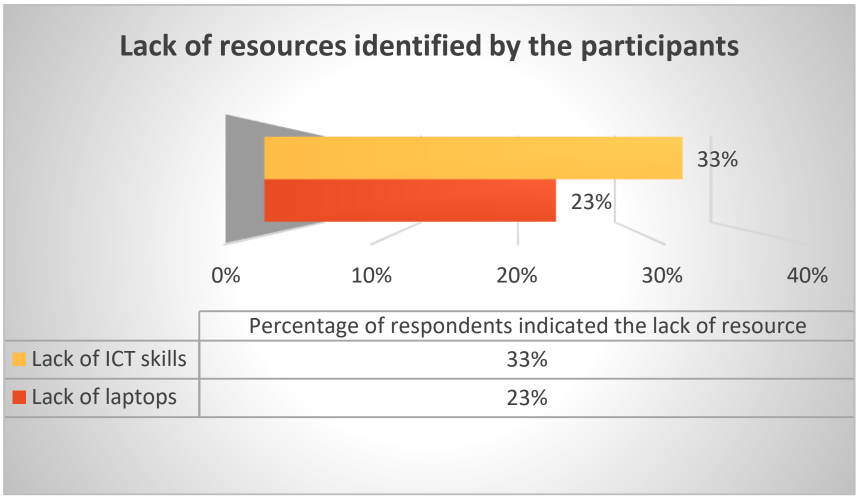


Figure 4.12: Lack of ICT resources

For this study to determine whether ICT has an impact on implementing risk management, the availability and utilisation of ICT resources are important. Twenty-three percent (23%) identified a lack of resources such as laptops (Figure 4.12). It is important to note that all the participants indicated that they had access to the laptops. However, this resource was identified as one of the lacking resources in the department. While some officials in the department had access to laptops, not all the officials responsible to implement risk management were able to operate remotely owing to the lack of laptops. This may have had a negative impact on performing risk management activities during the lockdown period. The organisation allocated data and virtual private network connections during this period, but this was not helpful to the officials who rely on desktops.

About 33% of the participants identified a lack of ICT skills to enable them to effectively use ICT in their daily risk management activities. These participants were risk champions from various business units. The common concern was on the SAP GRC system and the Excel template. The participants reported that they required technical skills to use the SAP GRC system. One of the reasons they were not fully utilising the system was their inadequate ICT skills. This came through the interview question on the challenges of using ICT in risk management. One participant, RC-D, indicated that lack of the skill to utilise the system might be a challenge. In support of that, RP_B highlighted the lack of understanding of the SAP GRC system while RP_C identified a lack of computer skills and capacity. In addition, as the risk register was developed using an Excel template, it had a level of automation that challenged the users. The risk practitioners who make up 17% of the participants provide training to the risk champions. The findings indicated that the trained users are not using the system fully for the risk practitioners to identify further training gaps.

4.3.7.2 Challenge 2: Technology and infrastructure

Among the building blocks outlined by IIF (2017) toward risk digitisation, is an emphasis that the IT infrastructure should be one of the priority areas that the organisation considers. Organisations must invest in their IT infrastructure to enable adequate support for business processes (Nadikattu, 2019). The conceptual framework for enterprise risk management identifies infrastructure as one of the fundamentals for the successful implementation of risk management. Some participants raised concerns regarding the old infrastructure owing to a lack of maintenance. The old infrastructure compromises the security of IT. One participant (RC_E) was of the view that it becomes difficult to rely on ICT if the organisation is not investing in IT infrastructure and maintaining the existing infrastructure. Furthermore, RO_15 advised that the aging IT infrastructure exposes the organisation to various IT security risks.

These concerns are clear indicators that the officials were willing to embrace innovation in risk management. However, the predicament caused by aged IT infrastructure impacts the full operation of IT. A challenge has been posed to the IT function of the organisation to involve itself in risk management activities to enhance the integration of ICT.

4.3.7.3 Challenge 3: Accessibility and reporting

Despite the benefits and usefulness of the SAP GRC system, all participants were vocal about the challenges the organisation faced during the reporting period. Twenty-three percent (23%) of the participants identified accessibility shortcomings to the SAP GRC system owing to network interruptions. If the users manage to access the network, the system takes longer to process their transactions. These participants further indicated that these challenges affect the reporting process negatively as they were unable to download and customise reports on time. Some of the participants alluded to the difficulties of not using the ICT reporting system daily which affects the effectiveness of reporting. This was owing to a lack of dedicated officials responsible for risk management in their respective units. Although there were risk champions appointed in various business units, risk management was viewed as an add-on function to their already full performance agreements. In the absence of the SAP GRC system, the users were forced to revert to the manual Excel register for reporting, which was time-consuming. The Excel reports limited the reporting process as they did not provide various management reports as opposed to the system.

These findings indicate that the organisation needs to invest in improving the reporting capability of the SAP GRC system. The delays during the reporting period will not be addressed unless the root cause of these challenges is dealt with. Furthermore, while the participants were highlighting these challenges, risks emerged from both the survey and interviews. These risks were identified with risk mitigation, as illustrated in Table 4.17.

Table 4.17: Proposed risk mitigations

RISK	**PROPOSED MITIGATION**
Inability to fully integrate ICT into risk management	• Adoption of technological approaches to support risk management.
Officials not adapting the innovative technologies	• Provision of ICT end-user training for all the risk champions and risk owners. • Continuous communication of technological changes
Information security risks	• Strengthen information security policy for implementation and monitoring. • Educate employees on information security.
Department not investing in IT infrastructure	• Funding to be made available for procurement and maintenance of IT infrastructure
Limitations to technology use	• Budget allocation for ICT resources/ equipment.

Kuzminykh, Ghita, Sokolov, and Bakhshi (2021) emphasise that risk management allows the organisation to identify procedures to mitigate the identified risks and inform management of the actions that need to be mitigated. To address the risks identified in Column 1 of Table 4.17 associated with the challenges of using ICT (Table 4.18), the research proposed mitigations that may need to be implemented. The proposed mitigations illustrated in Column 2 of Table 4.17 were informed by the outcomes of the survey and interviews where the participants recommended solutions for most of the challenges.

The next question, *4.2 How do you think these challenges can be addressed?* needed to understand whether the participants had a solution to the identified challenges. The participants proposed the following solutions: provision of adequate infrastructure, training and awareness, creation of ICT culture, and resource allocation. In support of the findings from the survey, the participants from the interviews highlighted that the department should consider the corrective measures illustrated in Table 4.18 to address the ICT-related challenges.

Table 4.18: Corrective measures

CHALLENGE	CORRECTIVE MEASURES
Resource allocation	• All officials must be provided with ICT working tools including data. • Regions and cluster offices are to be allocated dedicated risk practitioners with clear roles and that should be reflected in the structure. • Ensure that all officials are trained to develop ICT skills. • IT department to be visible in supporting the business with technological developments.
Training and awareness of ICT	• Regular training and awareness of ICT. • Creating a technology-minded institution – communication of the importance of risk management, training, and ensuring up-to-date IT infrastructure. • Motivate line function managers to embrace the use of ICT Risk Management and other ICT-related systems across the board. • Working towards moving to a paperless environment.
Infrastructure	• Procurement of new infrastructure. • Upgrade the existing infrastructure to strengthen the network and reduce downtime. • Perform regular software updates to protect departmental data and improve the stability of IT systems. • Develop an IT strategy to support business processes. • Develop a blueprint of how technology supports the departmental plan. • ICT must keep abreast of technological updates and new innovations.

The last question 4.3 *In your view, what would be the benefits of addressing these challenges?* sought to understand the benefits associated with the proposed corrective measures.

The participants listed the following as the benefits if all the measures were actioned:

- ease of access to the system which would result in efficiency.
- educated and aware workforce.
- better communication.
- infrastructure that can support the IT requirements and skilled workforce.

The responses to question 6 of the interview schedule, *What is the future of using ICT tools in risk management?* revealed that there is a future for technology in risk management. The participants opined that if all the identified challenges could be addressed, the use of ICT would improve resulting in effective implementation of risk management.

4.3.8 Establishing the validity of the findings

This study used triangulation to determine the validity and reliability of the research findings. The application of these concepts was defined in Chapter 3 where data source and method triangulation were adopted. Collecting data from the various categories of the participants such as risk practitioners, risk champions and IT officials provided the researcher with different perspectives. Moreover, the risk practitioners provided the study with a viewpoint on how they view the contribution of ICT in risk management from a risk management custodian perspective. This group also acknowledged that the risk champions and IT officials had a critical role to enhance the technology used in risk management. While the risk champions provided their perspective from a coordinating point of view, the findings from the risk champions confirmed the findings from the risk practitioners. The IT officials encouraged the adoption of ICT on risk management focusing more on how technology adoption would enhance the risk management process. The IT officials also affirmed the views of both the risk practitioners and the risk champions.

Over and above the data source, the method triangulation confirmed the credibility and dependability of the research findings. The survey findings were validated through interview findings. The interview results confirmed what was found through the interviews and further provided consistency in the study outcomes. Based on these two triangulation types, this study's validity was established. The next section provides theoretical elaboration.

4.4 INTERPRETATION OF RESEARCH FINDINGS

During data analysis, there were links between the literature reviewed and the collected data. Theoretical elaboration conceptualises the pre-existing concepts relevant to this study to comprehend the new insights.

4.4.1 Theoretical elaboration

It is critical to discuss these associations as they impacted ICT integration into risk management in the department. Table 4.19 highlights and discusses these associations. The discussion on the relationship between the literature review and the collected data influenced the development of the ICT-integrated framework. Section 4.3.2 elaborates on how the conceptual framework shaped this study.

Table 4.19: Links - literature and data

	LITERATURE	DATA	DISCUSSION
1	During strategic planning, ICT-related planning should be included to address issues of systems, knowledge, and information. ICT should be integrated into the risk management process where all ICT-related risks are managed. Furthermore, the literature suggests the integration of all risk management frameworks such as the ERM framework, COBIT, ISO, etc.	The department conducts IT risk assessment guided by the department's ERM framework in line with the strategic planning of the department with the support of the SAP GRC system. However, it is not clear to what extent are the IT risk managed.	This association is important for this study as it indicates an effort toward integrating ICT into risk management activities in the department. The fact that it is not clear the extent to which IT risks are managed suggests that there is room for improvement in this area. This association further provides a baseline for the proposal of the ICT integration framework for this study.
2	The literature identified a concern regarding the availability of resources to support IT-related activities.	The findings revealed that there are various ICT challenges such as data, ICT skills, networks, and limitations to access laptops. During the interviews with the participants, the availability of ICT resources was deemed a challenge as not all the risk champions in the department had sufficient access.	This association motivates a need that the department should invest in ICT resources, even more now that the organisation was affected by the COVID-19 pandemic. If all the users had access to laptops, data, and network connections among other things, it would have been possible to have all of them fully operational while they were working from home.

	LITERATURE	DATA	DISCUSSION
3.	Literature underscored the importance of the public sector in investing in financial resources for IT Infrastructure to support service delivery.	During the interviews, it was indicated that the department needed to invest more in its IT infrastructure to support IT integration into risk management. Funding for IT infrastructure was identified as a key aspect that needed to be prioritised.	The COVID-19 pandemic changed the operating landscape for the department. This provided an opportunity for the department to rely on technology. This is a motivation for the department to invest in IT infrastructure. The IT infrastructure is one of the critical assets for the department that may need to be accurately assessed in terms of risk management. While some of the officials were operating remotely during the lockdown, this was an opening for many IT security risks.
4.	Various researchers identified a list of ICT challenges such as the lack of adequate IT skills, insufficient financial resources, limited access, and IT knowledge.	Among the list of challenges identified during the survey and the interviews are the IT skills for the risk champions, limited access, network, IT security, and IT funding challenges to support integration.	This association is an indication that the department needs to prioritise investing in technology resources to support its business operations. While the participants were positive about the impact of using ICT to ensure the effectiveness of risk management, they acknowledged these challenges to be having a negative impact.
5.	The importance of identifying potential risks is in line with the advancement of technology.	The department identifies the IT risks using the ERM risk management framework.	This motivates a need to incorporate all aspects of IT risk identification into the proposed framework to integrate ICT into risk management.

4.4.2 Conceptual framework

The questions for this study were shaped to respond to the concepts relevant to the research question. The conceptual framework was developed from the existing theories, as indicated in Section 2.4. The three pillars of this framework include the factors that contribute to the effectiveness of the risk management process, how the organisation embraces the use of ICT in risk management, and the factors that contribute towards ICT adoption in risk management.

4.4.2.1 The factors contributing to the effectiveness of risk management

The officials involved in the implementation of risk management understand the factors (such as structure, governance, and process) contributing to effective risk management. While these aspects are in place in the organisation, the participants acknowledged that the need to integrate technology into their risk management activities was inevitable. The COVID-19 pandemic presented an opportunity to enhance the adoption of ICT in risk management. To exploit this opportunity, risk management initiated the creation of a technology-aware culture. The department has various technology platforms, including Microsoft Teams, for effective communication. The integration of ICT into risk management is a long-term goal that requires sufficient resources. The commitment and support from management to support this integration is essential while the risk champions have an active role as an extended arm of the risk management team. The key aspect is to ensure that the risk owners are part of the process moving forward. This will contribute to the effectiveness of risk management in the department.

4.4.2.2 How the organisation embraces technology in risk management

The participants in this study were embracing innovation at various levels. However, the risk management team is central to technology embracing in support of the implementation of the risk management process. The risk management team needs to acknowledge that, while the users may be willing to embrace technology, technology acceptance, and integration occur differently for different individuals. This is important as the risk practitioners are the custodians of risk management in the department. While the risk management team was taking the lead in introducing technology in risk management, other units were supporting them, including ICT units. The relationship between these units should be strengthened to improve ICT integration.

4.4.2.3 The factors contributing to ICT adoption

The participants were clear about the officials who were not adopting technology in risk management. The risk champions also acknowledged their difficulties in adapting to innovative technologies. The most critical innovation that needed to be prioritised in the department was the SAP GRC system. The use of this system can enhance the risk management process. There is a need to motivate the officials towards adoption to improve risk management processes. The risk champions work directly with the risk owners, which gives them a better chance to influence them. Moreover, a risk management team can influence management in various governance platforms such as risk and audit and committees together with the management structures.

The factors contributing to technology adoption were indicated to be both internal (issues that the participants had control over) and external (issues that the participants had no control over). The participants showed a willingness to address the internal factors they controlled, including the adoption of SAP GRC and other technologies used in risk management. The participants mostly emphasised the lack of commitment and competency regarding technology in their respective areas. Thompson and Glasø (2018) define the concept of competency as starting with knowledge, skills gained through formal education, and experience gained on-the-job training. This should be a starting point to build on for the risk practitioners. The risk management team should strive to develop competence by providing adequate training and awareness sessions on the SAP GRC.

Awareness sessions should ensure that management and other officials understand the importance of using technology and the benefits thereafter. This will assist the risk practitioners in identifying the best approach to educate those risk owners. The participants also alluded to the external factors that the department needed to prioritise. The risk management team must engage various stakeholders to address these factors as they have access to the organisation's management.

4.5 DELIVERABLE OF THE STUDY

The study is anticipated to contribute towards integrating technology into the day-to-day operations of risk management of the department. The next section illustrates the proposed model as a contribution to this study. Patiño, Solís, Yoo, and Arroyo (2018) proposed a risk management methodology similar to the recommended model.

4.5.1 The proposed model to integrate ICT into the risk management process

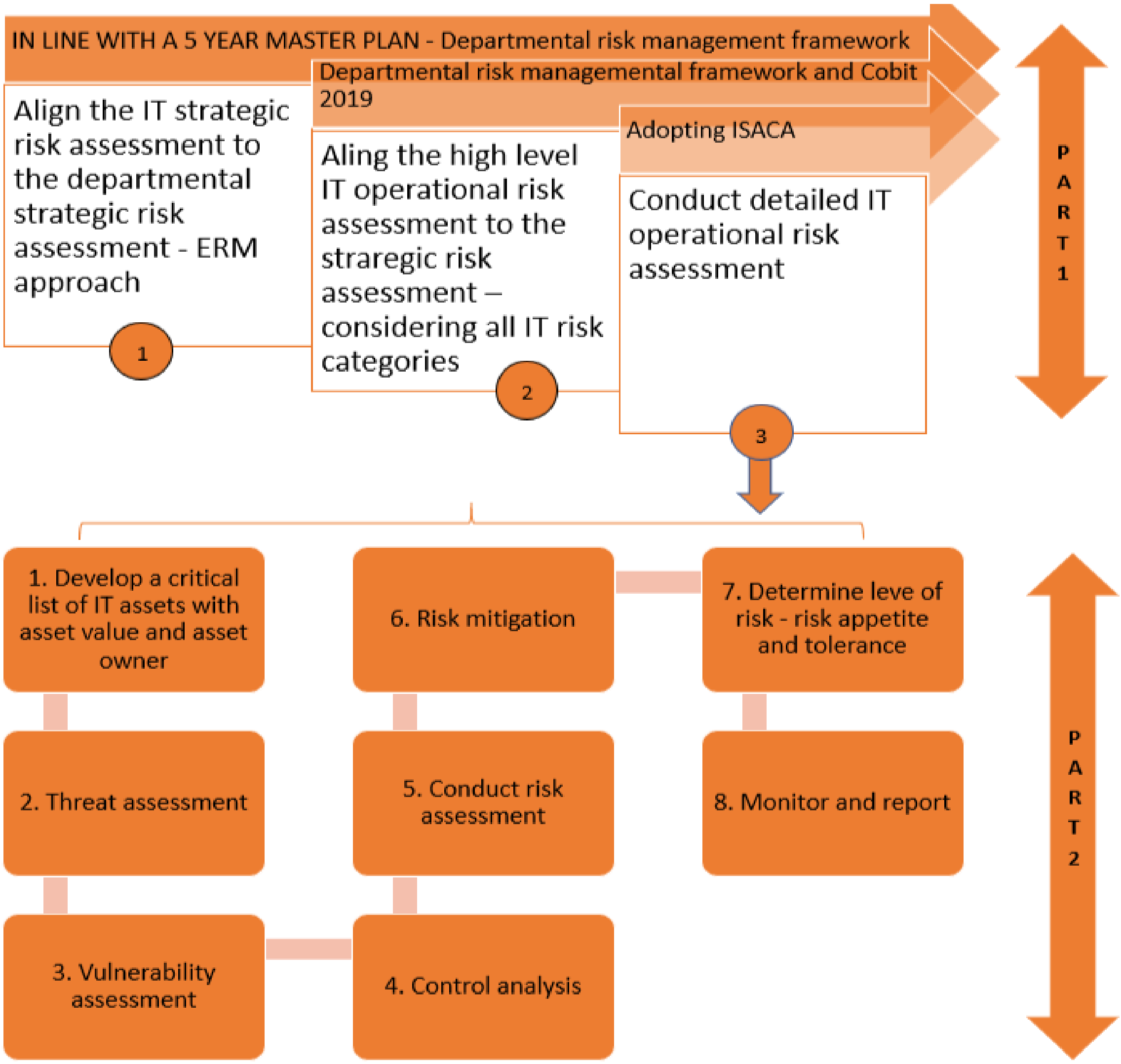

IN LINE WITH A 5 YEAR MASTER PLAN - Departmental risk management framework
Departmental risk managemental framework and Cobit 2019
Adopting ISACA
Align the IT strategic risk assessment to the departmental strategic risk assessment - ERM approach
1
Aling the high level IT operational risk assessment to the straregic risk assessment – considering all IT risk categories
2
Conduct detailed IT operational risk assessment
3
PART 1
1. Develop a critical list of IT assets with asset value and asset owner
2. Threat assessment
3. Vulnerability assessment
4. Control analysis
5. Conduct risk assessment
6. Risk mitigation
7. Determine leve of risk - risk appetite and tolerance
8. Monitor and report
PART 2

Figure 4.13: Proposed ICT integration risk model

Figure 4.13 demonstrates a proposed model for ICT integration into the risk management process in the public sector. This model adopts the process proposed for IT risk by the

Information Systems Audit and Control Association (Kassa and CISA, 2017). The proposed model was informed by the reviewed literature supported by the collected data. The literature emphasised a need to integrate various risk-related frameworks as discussed in Section 2.3. Based on the literature reviewed, all the risk management frameworks listed in Section 2.3 adopt a similar approach to implementing risk management. Lastly, the study findings based on the data collected, identified risks such as infrastructure and security which also contributed to the model.

Part 1 of the framework, as illustrated in Figure 4.13, commences with aligning to the existing departmental risk management framework where the risk assessments are conducted in line with a 5-year strategic plan. The IT master plan is aligned with the departmental strategic plan to support the objectives of the organisation. Following that, a detailed IT risk assessment should be conducted adopting the COBIT 2019 in line with the existing departmental risk management framework. Lastly, the new aspect that this proposal is introducing is the detailed IT risk assessment adopting the ISACA model. This is informed by the need to integrate all the risk management frameworks to improve the effectiveness of risk management in the public sector. Kassa and CISA (2017) provide a simple model to evaluate, manage, and follow up on assets, risks, and controls in the organisation to address the challenges that face IT professionals in providing assurance. The process that this model follows is detailed in part 2 of the framework. The following sections discuss each process of the framework for ease of implementation. As the SAP GRC emerged as one of the key IT assets for risk management from the collected data, these resources will be used as an example in unpacking the proposed model. Any allocation of values is at the researcher's discretion to understand the process based on the views of the participants. The organisation may have different values based on the practical assessment done together with the relevant stakeholders.

4.5.1.1 Develop a critical list of IT assets

Section 2.2.3 highlights the importance of IT risks which include IT assets and infrastructure. There are various definitions of assets from different standards and frameworks such as ISO/IEC 27005, COBIT, OCTAVE, NIST, and FAIR. Kuzminykh et al., (2021) define an asset as “anything that has value to the organisation and is necessary for achieving its objectives”. This definition is aligned with the definition of an asset in the COBIT framework. These assets include the server, people, and information systems among other things. This process allows the organisation to make risk-based decisions considering the confidentiality, integrity, and availability of the information technology assets (Kitsios et al., 2022). These concepts are defined as follows:

- Confidentiality is a process that ensures that information is only accessed by authorised individuals.
- Integrity is concerned about the accuracy and completeness of information – meaning protecting information from being altered whether intentionally or accidentally.
- Availability is about ensuring that the information on assets is accessible to the authorised users when it is required (Kitsios et al., 2022).

Kuzminykh, Ghita, Sokolov, and Bakhshi (2021) emphasise that the organisation identifies the critical assets to protect them from threats or vulnerabilities that may harm the confidentiality, availability, and integrity of the asset. When the organisation identifies the critical assets, security requirements for these assets should be identified (Kuzminykh et al., 2021). From the list of the ICT resources identified from data collection, SAP GRC qualifies to be one of the assets on the critical list. The system was identified as a critical resource that supports the organisation to implement risk management. Considering the nature of information captured on the system, this system should be risk assessed based on confidentiality, availability, and integrity.

Once the organisation identifies all the critical assets, the next phase is to allocate the owner and or custodian of the assets. The allocation of the risk or asset owner will ensure that people who are responsible for the assets take accountability for the risks associated with their assets. Kuzminykh et al., (2021) define the risk owner as the person responsible for the management of the risk associated with the asset, which makes the individual an asset owner. The risk or asset owner has the authority to decide on the priority of the assets listed on the critical list (Kitsios et al., 2022). In the case of the SAP GRC, the head of the risk management unit will be allocated as the risk owner with the head of IT taking an accountability role. The next step is to conduct the threat assessment.

4.5.1.2 Threat assessment

Threat assessment is an identification of the potential threats that may exploit the possible vulnerabilities and compromise security by causing harm to critical assets and analysing their impact. The potential threats may include system failure, and human interference among other things for the SAP GRC system. The threat can be measured using the metrics of high, medium, and low. These metrics are somehow aligned with the existing ones the department is using for the enterprise-wide risk assessment. Once the threats have been identified, the likelihood of them damaging the assets needs to be determined. The next step is to conduct a vulnerability assessment.

4.5.1.3 Vulnerability assessment

The vulnerability assessment should be conducted to determine the likelihood of the threats to vulnerability. For example, in the case of the SAP GRC system, an assessment for human interference from the users who are not trained needs to be assessed to determine how likely it is to affect the system. The vulnerability can be measured using the metrics of high, medium, and low. Once the vulnerability assessment is concluded, the assessment to determine the criticality of the vulnerability considering the consequences should be done.

4.5.1.4 Control analysis

The Information Technology Authority (ITA) (2017) indicated that the controls that the organisation has implemented or planned for implementation need to be identified and analysed to reduce the likelihood of a threat to the asset. The controls are informed by people, processes, and technology (ISO 27001:2022). In line with the ERM framework that is currently being implemented, the organisation can select different categories of control mechanisms such as preventive, detective, and corrective. Detective and preventive control detects the event and prevents it prior to manifestation, and if the event has occurred, the corrective control corrects the event.

4.5.1.5 Conduct risk assessment

The existing enterprise risk management framework in the departments requires the organisation to conduct risk assessment annually and to further identify emerging risks when the changes emerge. This approach applies to the IT risk assessment. Taylor (2015) argues that the organisation needs to conduct an accurate risk assessment to protect the information related to the assets. Shedden et al., (2016) further state that the identification of critical assets includes the identification of potential threats and vulnerabilities that the assets may be exposed to. To ensure accurate risk assessment, Figure 4.10 illustrates the process that should be adopted when conducting the enterprise-wide risk assessment. This process follows the process adopted from ISO 31000 standards. Considering that part 2 of the proposed framework focuses on IT assets, the process is supplemented by the approach of risk assessment suggested by ISO 27001. The first phase would be to establish the context in the scope to which the risks will be defined, such as internally and externally.

4.5.1.5.1 Establish context

According to the European Commission (2020), the external environment includes politics, natural, and technological factors, among others. Secondly, the internal factors may include objectives, strategies, and internal structures to list a few. These factors could be informed by strategic planning where the department's legislation should be considered both at a strategic and business unit level of an entity. The security context where the security parameters need to be determined with the mechanisms to protect the institution's information assets is established. Once the context has been established, the risk assessment should be conducted.

4.5.1.5.2 Risk assessment

The ITA (2017) and NIST (2018) define risk assessment as an adverse impact caused by an event resulting in a loss or degradation of the asset. This process assists the organisation to understand the loss that it may be exposed to in case the risk materialises. The ITA (2017) argues that conducting the IT risk assessment for assets requires multiple strategies to get the best possible outcomes. The risk assessment involves identifying, assessing, and evaluating the risk.

4.5.1.5.3 Identify, assess, and evaluate risks

The threats, vulnerability, and criticality assessments contribute to the identification of the risk aligned to the assets on the critical list. ISO 27001 argues that organisations define risks differently where some view it as ***risk = asset*threat*vulnerability*** while others see it as ***risk = asset + threat + vulnerability***. The two formulae simply mean that a threat exploits the vulnerability that causes a negative event and affects the asset resulting in business operations being affected. The risks need to be analysed and assessed.

The process of assessing the risk first requires the risk owner to understand the asset's value as discussed in Section 4.5.1.1 (Kassa & CISA, 2017; NIST, 2018). The asset value informs the impact and the likelihood of a threat to the asset. The asset value is calculated based on the confidentiality, integrity, and availability (Kitsios et al., 2022). This narration is illustrated in Figure 4.14.

Table 4.20: Calculation of the asset value

Sources: Source: Kitsios et al., 2022

	ASSET NAME	C	I	A	MAX	CATEGORY
Information	Network drive	3	2	3	3	High
People	Risk champions	3	3	3	3	High
Physical	Server	2	3	2	3	High
Software	SAP GRC	4	3	3	4	Critical

LEGENDS				
C- Confidentiality	1 - Low	2 - Medium	3 - High	4 - Critical
I - Integrity	1 - Low	2 - Medium	3 - High	4 - Critical

A - Availability	1 - Low	2 - Medium	3 - High	4 - Critical
	1 - Low	2 - Medium	3 - High	4 - Critical

Table 4.20 shows the assets listed on the critical list of assets categorised per asset group. Each of these assets is determined a value considering the confidentiality (C), the integrity (I), and the accessibility (A) of the asset (Kitsios et al., 2022). The value of each asset uses a rating between 1 to 4 as illustrated in the legend where 1 represents low, 2 represents medium, 3 represents high and 4 represents critical. While the value of the asset considers all three aspects, the maximum score is used as a value for the specific asset. An example is that for the SAP GRC that is part of the software group, the value allocated to the asset is a 4 - this represented the confidentiality but is also a maximum value hence the asset value for SAP GRC is critical with a score of 4. Secondly, an impact that may be caused by the breach and the likelihood of the breach for confidentiality, integrity, and availability is determined using the formula risk = impact and likelihood. Table 4.21 illustrates the determination of the impact and Table 4.22 illustrates the likelihood of the event.

Table 4.21: Determining an impact

DETERMINING IMPACT		
Rating	Level of an event	Description
1	Insignificant	Critical systems not operational for not more than 4 hours
2	Minor	Critical systems not operational for between 5 to 11 hours
3	Moderate	Critical systems not operational for between 12 to 24 hours
4	Major	Critical systems not operational for between 1 & 2 days
5	Catastrophic	Critical systems not operational for greater than 2 days

Table 4.22: Determining the likelihood

DETERMINING LIKELIHOOD		
Rating	**Level of an event**	**Description**
1	Rare	The event may occur within the next 5 to 10 years
2	Unlikely	The event may occur within the next 2 to 5 years
3	Moderate	The event is certain to occur within the next 18 to 24 months
4	Likely	The event is certain to occur within the next 12 to 18 months
5	Almost certain	The event is certain to occur within the next 12 months or has already occurred

Table 4.21 and Table 4.22 provide guidance for determining the impact and likelihood of an event occurring (Kitsios et al., 2022). The scale of 1 to 5 utilised for evaluating the risk is in line with the scale adopted in the departmental risk management framework. The meaning of each rating for both impact and likelihood is provided in a description column. This is the process of assessing and evaluating the risk and it will inform you whether a mitigation strategy is required or not. As the SAP GRC asset value has been assigned 4, the assumption is that a risk of unauthorised access to the system has been identified. The risk owner assigns the impact of this risk to a 5 and the likelihood to a 4. Calculating the severity of a risk is done by multiplying impact and likelihood. This means for SAP GRC: Severity = Impact (5) *Likelihood (4) equals 20 which is very high, as illustrated in Table 4.23.

Table 4.23: Risk severity description

Source: The Information Technology Authority (ITA) (2017)

RISK SEVERITY DESCRIPTIONS		
Qualitative value	**Quantitative value**	**Description**
Very high	21 - 25	An event may have multiple severe or catastrophically adverse effects on organisational operations.
High	16 - 20	An event may have severe or catastrophic adverse effects on organisational operations.
Moderate	10 - 15	An event may have serious adverse effects on organisational operations.
Low	6 - 9	An event may have limited adverse effects on organisational operations.
Very low	1 - 5	An event may have negligible adverse effects on organisational operations.

4.5.1.5.4 Mitigate the risk

To mitigate the risks, the organisation should understand that all the assets have some level of value. However, owing to budgetary and time constraints, the risks need to be prioritised in line with cost-benefit analysis (Kitsios et al., 2022). For effective management of risk, the risks should be identified and evaluated for each asset. The risk severity score, as demonstrated in Table 4.23, will inform the level of mitigation strategy that the risk requires. This will help prioritise and allocate resources to mitigate the risks.

Kitsios et al., *(*2022) advise that managers should consider four basic mitigation responses referring them to treatment options when they are managing their priority risks. Figure 4.14 illustrates the mitigation responses and when they should be selected.

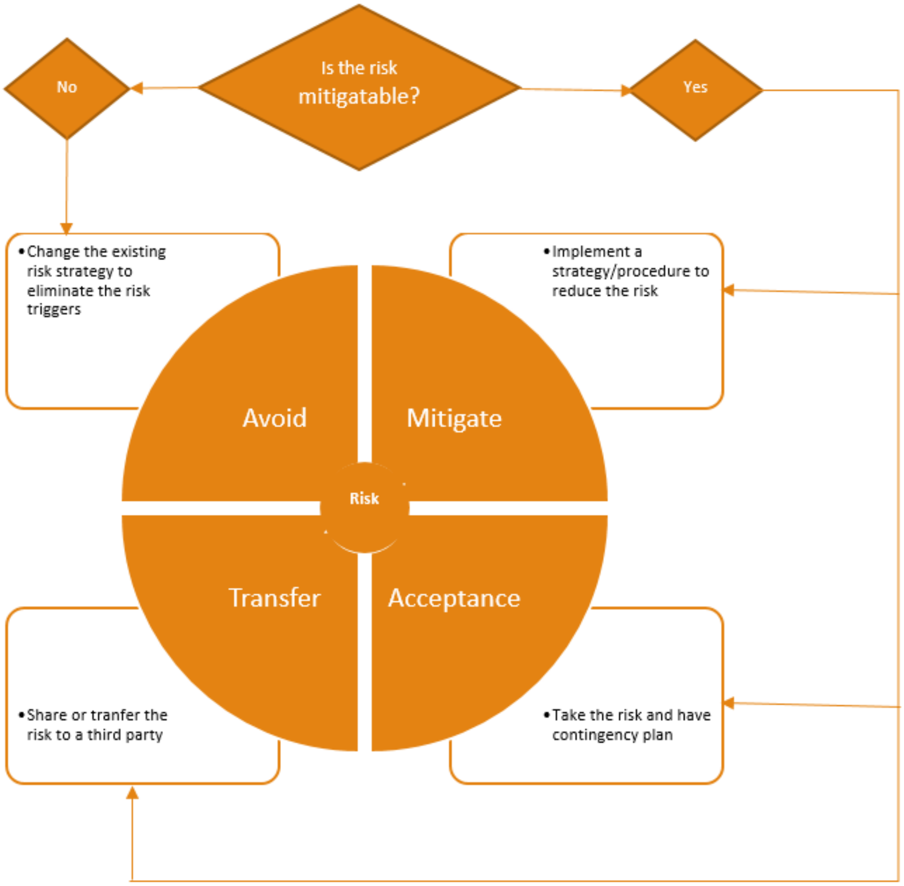

Is the risk mitigatable?
No
Yes
•Change the existing risk strategy to eliminate the risk triggers
•Implement a strategy/procedure to reduce the risk
Avoid
Mitigate
Risk
Transfer
Acceptance
•Share or tranfer the risk to a third party
•Take the risk and have contingency plan

Figure 4.14: Response strategies

These responses (risk avoidance, mitigation, transfer, and acceptance) are defined with examples using the SAP GRC system as a critical resource in this study as follows:

4.5.1.5.4.1 Avoidance

Risk avoidance is about management deciding to minimise the organisation’s exposure to risk. In the case where the organisation is faced with a risk of data manipulation, the department may implement an audit trail report. Further, read or write permission is granted to the users. The risk champions and owners may be granted rights to the system – these rights can allow them to read only in some areas while they can write in the risk areas allocated to them.

4.5.1.5.4.2 Mitigation

Mitigation is an action taken by management to reduce the impact or likelihood of the risk. If the risk of limited access to the work place due to disaster is identified, a virtual private network connection should be implemented as a strategy to allow access to the system while working offsite.

4.5.1.5.4.3 Accept

Risk acceptance is defined as a process where managers must decide formally (documented) to accept the risk and implement a contingency plan due to the cost implications. The department should accept the risk that some of the risk champions may not update the system reports promptly. The risk management team should have practitioners readily available to update the system.

4.5.1.5.4.4 Transfer

Risk transfer is a process to move the risk (either fully or partly) from the risk owner's responsibility to the third party. An asset owner can transfer the risk of a failure of a server to the departmental IT department as the custodian of the asset.

The overall intention of identifying the risks is to ensure that they are being mitigated. However, the response strategy assists management to make an informed decision without compromising the organisation or using the resources unnecessarily. The participants indicated they monitored the mitigations formally quarterly in line with the departmental risk appetite and tolerance level framework. This process has been integrated into the SAP GRC system for the department. Management needs to determine if they need to revise their plans by tracking the effectiveness of the mitigations and testing them against the acceptance level, as discussed in the next section.

4.5.1.5.4.5 Determine the level of a risk

The impact and probability rating scale defined in the existing risk management framework can be utilised as the framework accommodates IT-related risks. The department has developed the risk and appetite framework for enterprise risks. This framework (which also includes IT risk appetite and tolerance levels) holds the management accountable to determine the appetite and tolerance levels for each objective in their branches (DWS, 2021a). This agrees with the sentiments of Martens and Rittenberg (2020) where it is emphasised that management has a responsibility to develop appetite levels and cascade it down to the organisation. Martens and Rittenberg (2020) further maintain that defining appetite levels assists the organisation to make informed decisions. IT-related risks are part of the enterprise, hence the organisation needs to define both appetite and tolerance levels for them.

Martens and Rittenberg (2020) underscore the importance of the objectives in setting up risk tolerance. This means the most critical objectives would be assigned a low tolerance level. This is supported by the departmental risk management framework where fraud and corruption have been allocated a zero-tolerance level (DWS, 2021b). Fraud and corruption may occur owing to the security compromise of the supply chain management systems. For the example used in this study, unauthorized access to the SAP GRC may be allocated a low appetite score. Further, once the risk has been allocated low tolerance, the organisation needs to allocate the greater part of the resources to maintain the risk within the lower range (Martens & Rittenberg, 2020). The process needs to be formally communicated with the risk owners. The communication process allows the risk owners to keep track of their risk assessments and monitor the implementation of the mitigation strategies. According to Nadikattu (2019), monitoring the progress of the mitigations includes tracking the risk on the register, identifying emerging risks, and evaluating risk process effectiveness throughout the cycle, which is the case in the department. This process is integrated into the SAP GRC system for the department.

4.5.1.5.4.6 Monitor and report

While the monitoring of the risks has been discussed during Step 3 – Conducting risk assessment, and reporting these risks should be done. Mazumder and Hossain (2018) argue that risk reporting, while risk reporting is key, can be perceived as both positive and negative by various stakeholders. Disclosing positive risks can boost the organisation’s confidence while resulting in the stakeholders having trust in the institution. However, stakeholders may lose their trust when the negative risks are disclosed as they are perceived as negative. Mazumder and Hossain (2018) further highlight the countries where risk reporting is either voluntary or compulsory and South Africa is among the countries where corporate risk reporting is compulsory. Bryce, Chmura, Webb, and Stiebale (2019) conclude that human behaviour plays a role in reporting the risks after utilising innovation to determine trends around risk reporting. During data collection, the participants highlighted that various business units or risk owners fail to report on the progress of their risk mitigations on time. This has a negative impact on the quarterly reporting to various governance structures. As discussed in sub-theme 3.1 (Value of ICT resources), the SAP GRC system has an automated reporting functionality that warns the risk owners of their overdue mitigations. Various management reports can be utilised for different reporting structures for various purposes. The department should fully utilise these capabilities to ensure effective reporting.

The collected data yielded consistent findings through multiple data sources such as the survey and the interviews. Based on the findings of this study, the researcher views the proposed model to have the potential to improve the effectiveness of risk management in the public sector. A key element identified from the survey and the interviews is that IT risk management is conducted using the generic risk management framework. This formed a baseline for the proposed model to integrate ICT to support risk management. Over and above the model, the findings provided a view of the ICT challenges, availability, and use of ICT that will assist the implementation of the proposed technology model.

To implement the recommendations of this study, the risk management team should be mindful of how the stakeholders in the department perceive the innovation. The users (stakeholders) need to be convinced of the benefits of moving toward the direction of integrating technology in their routine risk management activities. The level of acceptance of integrating technology into risk management may be low. However, a change of mind-set may be seen if they understand the benefits brought by technology. Involving them throughout the process of introducing the change will address their reluctance to change, which might result in easy adoption.

4.6 FINAL REMARKS

4.6.1 Emotions that emerged from the interviews and their interpretations

Out of the seven questions that were asked during the interviews, three questions received considerable attention from the participants and triggered more discussions. These questions were:

- Question 4: Is ICT playing an effective role in implementing risk management activities?
- Question 5: What challenges do you have in using ICT tools in risk management?
- Question 6: What is the future of using ICT tools in risk management?

The participants showed various emotions in line with these questions, as illustrated in Table 4.24 as numbers 1 to 3. These emotions were observed through the interview questions and recorded on the template document for the thematic analysis.

Table 4.24: Emotions from the interviews

RESEARCH QUESTION RELATED TO THE EMOTIONS	EMOTIONS	NO. OF PARTICIPANTS
1. Is ICT playing an effective role in implementing risk management activities?	Unsure	2
	Uncomfortable	1
	Confident	6
	Hopeful	6
	Frustrated	1
2. What challenges do you have in using ICT tools in risk management?	Stressed	10
	Frustrated	10
3. What is the future of using ICT tools in risk management?	Positive	7
	Appreciation	7
	Looking forward	3
	Willingness to embrace	2
	Reluctant	1
	Concerned	1

The emotions outlined in Table 4.24 were mostly positive as illustrated with a blue-colour coding. Most of the participants perceived ICT to have a positive contribution to the effectiveness of risk management regardless of the ICT challenges. Sixty percent (60%) of the participants were confident and hopeful that if the organisation were to address the identified challenges, using ICT can improve the effectiveness of risk management even further. An interesting view is that most of these participants were from the risk management unit. There were a few risk champions who were unsure, uncomfortable, and frustrated. With the drive and willingness of the risk management team, the aspect of doubt from the risk champions may be positively influenced.

The issue of the challenges facing the use of ICT dominated as all the participants were vocal about these challenges. While the participants were frustrated and stressed by these challenges, how they perceived the future of using ICT was positive. The willingness to embrace technology, the appreciation of what had been made available to them and looking forward to the innovations outnumbered the concerns and reluctance.

4.7 CONCLUSION

The goal of this study was to determine how ICT contributes to the effectiveness of risk management in the department. The findings presented in this chapter were informed by the survey and interviews conducted. The findings have ascertained that ICT influences the effectiveness of risk management. The themes from data collection were presented in line with the study's research problem. These themes confirmed the literature review. Furthermore, this chapter not only identified the challenges affecting the integration of ICT to risk management but proposed corrective measures to improve the risk management process.

CHAPTER 5: RECOMMENDATIONS AND CONCLUSION

The layout of this chapter is diagrammatically presented in Figure 5.1. This chapter outlines the introduction in Section 5.1 followed by addressing the research objectives and questions in Section 5.2. The summary of the study is presented in Section 5.3 followed by the recommendations in Section 5.4 and the research contribution in Section 5.5. Lastly, Section 5.6 outlines the future research with the researcher's personal reflections in Section 5.7, and finally, the conclusion follows in Section 5.8.

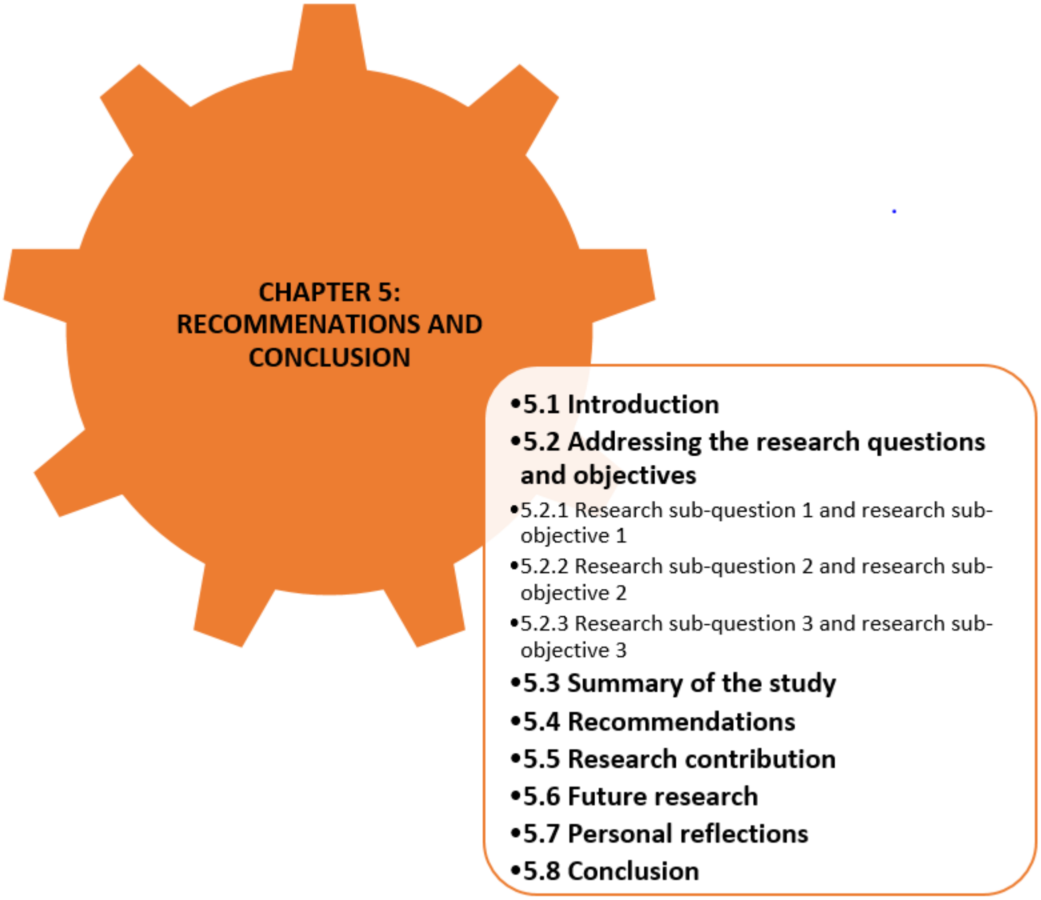

CHAPTER 5: RECOMMENATIONS AND CONCLUSION
•5.1 Introduction
•5.2 Addressing the research questions and objectives
•5.2.1 Research sub-question 1 and research sub-objective 1
•5.2.2 Research sub-question 2 and research sub-objective 2
•5.2.3 Research sub-question 3 and research sub-objective 3
•5.3 Summary of the study
•5.4 Recommendations
•5.5 Research contribution
•5.6 Future research
•5.7 Personal reflections
•5.8 Conclusion

Figure 5.1: Chapter 5 layout

5.1 INTRODUCTION

This chapter provides the research with recommendations based on the study findings and the conclusion made thereafter. To conclude this study, this chapter provides a summary of the study, a determination of whether the research questions were answered successfully, a conclusion, and recommendations based on the research findings. Lastly, this chapter provides the reflections of the researcher considering personal reflections, strengths and weaknesses of integrating ICT in risk management, implications for future research, and concluding remarks.

5.2 ADDRESSING THE RESEARCH QUESTIONS AND OBJECTIVES

This study aimed to examine the impact of ICT on the effectiveness of risk management in the public sector. The research argument of this study is centred around the ICT not being fully integrated into risk management. Specifically, this study aimed to address the main research objective:

> *"To investigate the technology model that the organisation ought to adopt to integrate ICT into risk management process in the public sector".*

This objective was achieved through the main research question:

> *"How should ICT be used in an organisation so that it has a positive impact on the effectiveness of risk management?".*

The main research question and main research objective were supported by the secondary research questions (research sub-objectives and research sub-questions).

The qualitative survey and the case study adopted in the research methodology aimed to achieve the three research sub-objectives and further contribute towards answering the main research objective and question in Section 1.4.1. The research sub-objectives are illustrated together with the research sub-questions in Figure 5.2, mapping the sub-objective to the related questions from both the survey and the interviews.

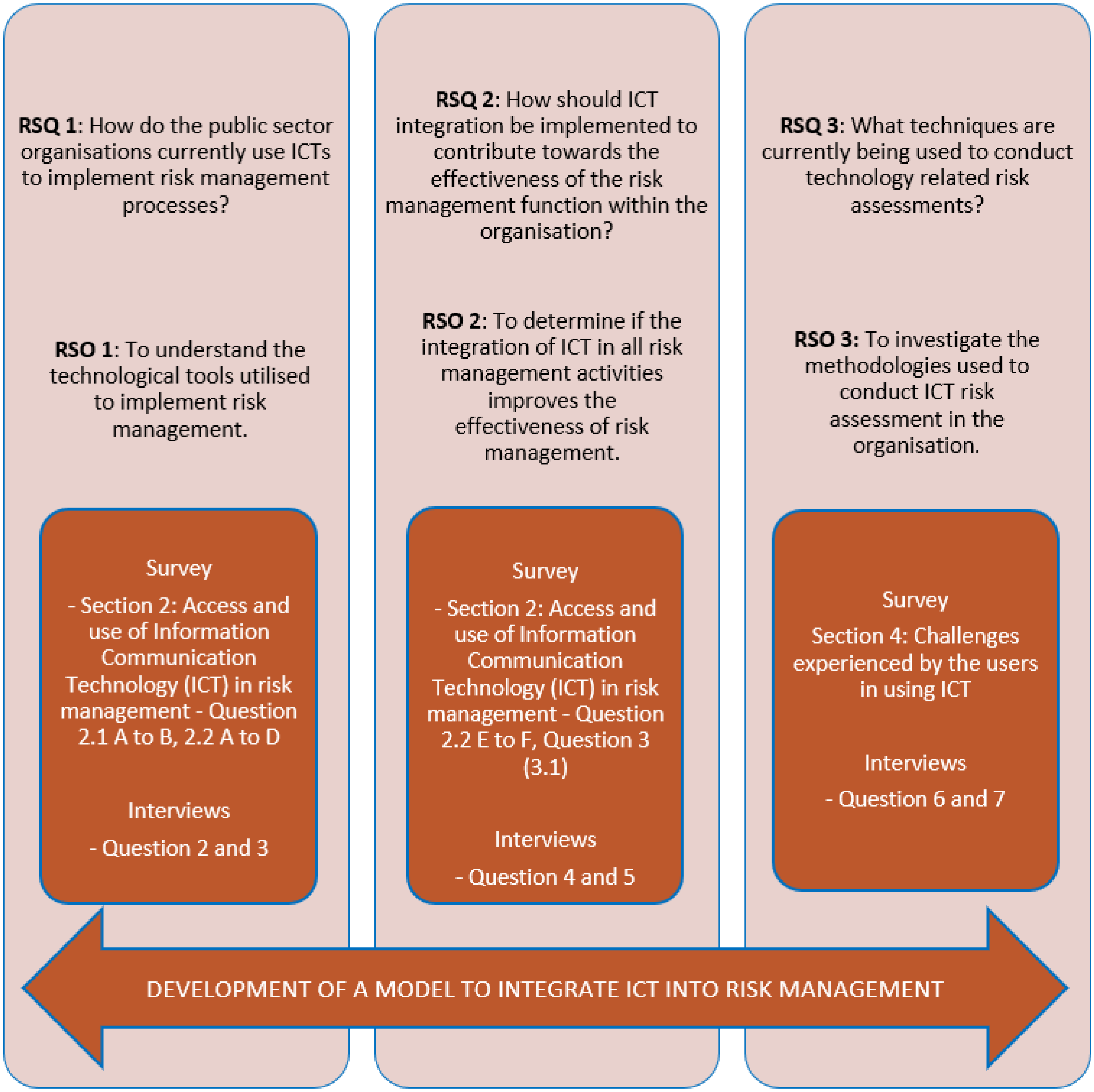

RSQ 1: How do the public sector organisations currently use ICTs to implement risk management processes?
RSO 1: To understand the technological tools utilised to implement risk management.
Survey
- Section 2: Access and use of Information Communication Technology (ICT) in risk management - Question 2.1 A to B, 2.2 A to D
Interviews
- Question 2 and 3
RSQ 2: How should ICT integration be implemented to contribute towards the effectiveness of the risk management function within the organisation?
RSO 2: To determine if the integration of ICT in all risk management activities improves the effectiveness of risk management.
Survey
- Section 2: Access and use of Information Communication Technology (ICT) in risk management - Question 2.2 E to F, Question 3 (3.1)
Interviews
- Question 4 and 5
RSQ 3: What techniques are currently being used to conduct technology related risk assessments?
RSO 3: To investigate the methodologies used to conduct ICT risk assessment in the organisation.
Survey
Section 4: Challenges experienced by the users in using ICT
Interviews
- Question 6 and 7
DEVELOPMENT OF A MODEL TO INTEGRATE ICT INTO RISK MANAGEMENT

Figure 5.2: Sub-objective mapping

The sub-objective mapping in Figure 5.2 illustrates the data instruments utilised to respond to each research question.

5.2.1 Research Sub-Question 1 (RSQ 1) and Research Sub-Objective 1 (RSO 1)

Research sub-question 1 (RSQ 1): How do public sector organisations currently use ICTs to implement risk management processes?

Research sub-objective 1 (RSO 1): To understand the technological tools utilised to implement risk management.

To achieve the research sub-question 1 and research sub-objective 1, the questions on access to information from the survey were asked (Annexure F, Section 2, 2.1 A to B, 2.2 A to D). The findings uncovered that there was reasonable access to ICT resources to support risk management activities. This was verified through interviews (Questions 2 and 3) where participants were clear on the effective role played by ICT in risk management. The fundamental issues that emerged from this objective can be summarised as follows:

- ICT is used to support the implementation of risk management processes at the DWS. However, there are detrimental factors that result in ICT not being fully utilised.
- The department is in the process of rolling out the SAP GRC system which is a fundamental tool that supports the risk management process; however, the system is not utilised by all relevant stakeholders to its full capabilities.
- There is a need to raise awareness of the rollout of the SAP GRC system and its benefit to all stakeholders involved.

5.2.2 Research Sub-Question 2 (RSQ 2) and Research Sub-Objective 2 (RSO 2)

Research sub-question 2 (RSQ 2): How should ICT integration be implemented to contribute towards the effectiveness of the risk management function within the organisation?

Research sub-objective 2 (RSO 2): To determine if the integration of ICT in all risk management activities improves the effectiveness of risk management.

To achieve research sub-question 2 and sub-objective 2, the questions on the importance and usefulness of using ICT in risk management were asked (Annexure F, Section 2, Questions 2.2 E to D) and Question 3.1 from the survey. The findings confirmed that ICT was useful in supporting risk management and had the potential to improve the process even further. This was verified through interviews (Annexure G, Questions 4 and 5). The interviews confirmed the effective role played by ICT in risk management, emphasising that the challenges be addressed to realise the benefits of integrating ICT into all risk management activities. The fundamental issues that emerged from this objective can be summarised as follows:

- To a certain extent, the integration of risk management can improve its effectiveness. It is concluded that integrating ICT into risk management enhances efficiency in risk management. Proactive risk reporting is one of the indicators of effective risk management. The SAP GRC system has a reporting competency that may need to be intensified.
- The department should fully utilise the risk proposal capability of the SAP GRC to eliminate face-to-face risk assessment workshops in the future. This will save the department time and costs.

5.2.3 Research Sub-Question 3 (RSQ 3) and Research Sub-Objective 3 (RSO 3)

Research sub-question 3 (RSQ 3): *What techniques are currently being used to conduct technology-related risk assessments?*

Research sub-objective 3 (RSO 3): *To investigate the methodologies used to conduct ICT risk assessment in the organisation.*

To achieve research sub-question 3 and sub-objective 3, the questions on the challenges facing the participants (Annexure F, Section 4, Questions 4.1 to 4.3) from the survey were asked. The findings were verified through interviews (Annexure G, Questions 6 and 7) on the future of ICT in the department and the final view of the participants. While it was evident that the department conducted the IT risk assessment annually at a strategic level, it was concluded that strengthening the integration of ICT would bring opportunity for the IT assets risk assessment to be done. Nevertheless, there was no clear indication of the formal process where risk assessment was conducted for the IT assets. Having an appropriate risk assessment approach ensures accountability in managing IT risks. Therefore, there is a need to conduct an IT risk assessment for all the critical IT assets in the department.

Overall, the research confirmed that ICT plays a critical role in supporting the implementation of risk management. Furthermore, the findings guided the development of the prosed model to integrate ICT into risk management. However, the findings also indicated the various challenges and risks affecting the integration of ICT to enhance the effectiveness of risk management functions. The next section outlines the summary of the study.

5.3 SUMMARY OF THE STUDY

The sub-question mapping was developed to demonstrate how the main research question was answered. The findings revealed that there was reasonable access and utilisation of ICT in risk management. Furthermore, the interviews validated the state of ICT access and availability in the department, specifically to support risk management. Secondly, the findings confirmed that ICT was indeed useful in risk management and that it had the potential to improve the process even further. The interviews confirmed the contribution of ICT in risk management emphasising that the challenges should be addressed for the department to realise the benefits of integrating ICT into risk management. Lastly, while it was clear that the department conducted IT risk assessment from a prominent level, it was not clear to what extent IT risk assessment was conducted. The study concluded that strengthening the integration of ICT would bring an opportunity for the IT assets risk assessment to be done.

The research confirmed that ICT plays a critical role in supporting the implementation of risk management. However, the findings also indicated the various challenges and risks affecting the integration of ICT to enhance the effectiveness of risk management functions. Section 5.5 discusses the recommendations based on the findings.

5.4 RECOMMENDATIONS

The analysis of the findings led to the recommendations in line with the objectives set out in Chapter 1, as illustrated in Table 5.1.

Table 5.1: Recommendations

SUB-RESEARCH QUESTION	SUB-OBJECTIVE	RECOMMENDATION
RSQ 1: How do public sector organisations currently use ICTs to implement risk management processes?	RSO 1: To understand the technological tools utilised to implement risk management.	Considering that the ICT tools are utilised in the organisation, it could be useful to: • Conduct a Strength, Weakness, Opportunity, and Threat (SWOT) analysis to understand internal and external factors affecting the use of ICT in risk management. • Develop actions to address the areas of weaknesses and threats to mitigate the challenges identified. This will provide a strong sense of the extent to which the ICT tools are utilised.
RSQ 2: How should ICT integration be implemented to contribute towards the effectiveness of the risk management function within the organisation?	RSO 2: To determine if the integration of ICT in all risk management activities improves the effectiveness of risk management.	The strengthen the gaps identified in Chapter 4, the following are recommended: • Digitise the process of risk identification and assessment. • Build capacity to support the digitisation process.
RSQ 3: What techniques are currently being used to conduct technology-related risk assessments?	RSO 3: To investigate the methodologies used to conduct ICT risk assessment in the organisation.	To optimise the IT risk assessment that is currently being done through the generic risk management framework, the organisation should: • Conduct IT risk assessment for all critical IT assets using the proposed model.

5.4.1 Use of ICT tools to implement risk management process

As demonstrated in Chapter 4, ICT tools are made available to most officials for use in performing risk management activities, although challenges have been identified. The recommendations are as follows:

To intensify the use of technology in risk management, the department needs to conduct a SWOT analysis to understand the internal and external factors affecting the use of ICT in risk management. The internal analysis will help the organisation understand the SWOT. Once the analysis has been conducted, the department should develop action measures to address the areas of weakness.

For the effective rollout of the risk management IT system (SAP GRC), the department should develop a roadmap allocating time frames for various activities to implement the system. The training needs analysis should be conducted to understand the training gaps owing to a lack of skills and competency. The training should be tailored to accommodate all the needs identified by the risk champions and extended to all the risk owners. The leadership of risk management should have clear communication with the top management of the department to ensure that the management takes the lead in adopting technology in risk management. Once the management of the organisation fully embraces the use of technology and understands the benefits, it will become easy for the rest of the department to follow suit. The risk management team needs to work with the IT business unit to ensure the effective management of any information and technology governance issues.

5.4.2 Fully integrate ICT in all risk management activities to improve the effectiveness of risk management

The recommendations for the use of ICT in risk management sets a platform for the department to embrace the technology change. The department should fully digitise the process of risk identification, assessments, and reporting. In addition, the department needs to invest in various technology tools for conducting risk identification and assessment to replace traditional approaches like face-to-face workshops. The existing risk management IT system can identify, assess and monitor emerging risks quarterly. The department needs to build capacity and take advantage of this system. Extensive training should be provided to the risk champions to fully understand how to use this functionality and the benefits thereof. Once the risk champions are well trained in utilising the system, the training needs to be rolled out to all the risk owners in a phased approach. Training should consider the adoption curve in the sense that people do not adapt to innovation at the same time. The training intervention needs to be tailored to accommodate the individual user's ability to adapt.

5.4.3 The approach to conducting ICT risk assessment in the organisation

Over and above the strategic and high-level risk assessment that the department performs annually, the department should conduct an IT risk assessment for all critical IT assets. The participants highlighted various challenges around confidentiality, integrity, and the availability of the SAP GRC system. Considering the information security challenges, the department should consider adopting the proposed model as illustrated in Chapter 4, Figure 4.13.

5.5 RESEARCH CONTRIBUTION

To the best of the researcher's knowledge, this study provided new knowledge in the field of risk management in the public sector. This is the first study to explore the integration of ICT into risk management within the sector. This study, therefore, contributes an in-depth understanding of how ICT impacts the effectiveness of risk management. Furthermore, the challenges affecting the adoption of ICT in risk management with corrective measures were documented. These challenges, if addressed, have the potential to improve risk management. More importantly, the conceptual framework developed for this study assisted in the development of the proposed model that the public sector can adopt to support risk management in the public sector.

5.6 FUTURE RESEARCH

For future research, an investigation into the extent to which the public sector is investing in technology to support the implementation of risk management should be conducted. Considering the shift brought about by the COVID-19 pandemic on how organisations operate in cases such as remote working, public sector organisations should allocate sufficient funding for the latest technologies. A further investigation to determine the impact of risk management on organisational performance, while considering the integration of ICT into risk management in the public sector, may need to be conducted. Lastly, the status to which the public sector is conducting a risk assessment for IT assets should be investigated. This may include the practical guidance to implement the proposed model to integrate ICT into risk management.

5.7 PERSONAL REFLECTIONS

This study was inspired by the passion the researcher has for risk management in the public sector. The researcher has been working in this environment for more than ten years seeing risk management maturing from one stage to another. The main driver of this research was the fact that the public sector is making strides in implementing risk management, but the researcher believes that risk management is not yet making the difference it was intended for. It was for this reason that the researcher decided to investigate how integrating the use of technology would assist the process. An interesting environmental change was brought to the public sector by the COVID-19 pandemic. This pandemic changed business operations in the public sector and throughout the country. While the 4IR was reshaping the current government business (Nalubega & Uwizeyimana, 2019), COVID-19 pressurised the public sector to make faster strides in embracing technology.

Lessons learnt in terms of the study include the realisation that ICT access and knowledge are key factors that affect the use and impact of ICT usage in risk management. While these areas needed some improvements, there were visible strengths identified in using technology in risk management. Furthermore, the importance of removing the self from the investigation and allowing the views of the participants gave the researcher a distinct perspective and added shape to the research.

5.8 CONCLUSION

The main purpose of this study was to determine how the users view the impact of using ICT influences the effectiveness of risk management in the public sector. It was confirmed that ICT plays a significant role in implementing effective risk management. This was proven through the emotions, experiences, and feelings of the users involved in daily risk management activities. However, a variety of challenges were assumed to harm the integration of ICT in risk management.

The sub-research questions set in Chapter 1 were thoroughly investigated. This resulted in the main research question of whether the use of ICT to implement risk management has an impact on the effectiveness of risk management being answered successfully. An assumption was that, if the users have access to ICT resources and were willing to embrace using ICT, there should be a positive influence on risk management. The research findings have confirmed that assumption. The researcher, therefore, believes that the attitude toward embracing technology in risk management is important. With the change of attitude with the willingness to adopt technology, the organisation should be able to realise the benefits of integrating ICT into risk management.

REFERENCES

Adom, D., Hussein, E.K. & Agyem, J.A. 2018. Theoretical and conceptual framework: Mandatory ingredients of a quality research. *International journal of scientific research*, *7*(1), 438-441. Available at: https://www.researchgate.net/publication/322204158_Theoreticaland_Conceptual_Framework_Mandatory_Ingredients_Of_A_Quality_Research [Accessed:14 June 2021].

Adu, P. 2019*. A step-by-step guide to qualitative data coding*. New York: Routledge.

Ahmeti, R. & Vladi, D. 2017. Risk management in public sector: A literature review. *European Journal of Multidisciplinary Studies, 2*(5): 190-196.

Akatov, N., Mingaleva, Z. & Klačková. 2019. Expert technology for risk management in the implementation of QRM in a high-tech industrial enterprise*. Management Systems in Production Engineering,* 27(4): 250-254.

Ako-Nai, A. & Singh, A.M. 2019. Information technology governance framework for improving organisational performance. *South African Journal of Information Management,* 21(1): 1-11*.*

Algheriani, N.M.S., Majstorovic, V.D. & Kirin, S. 2019. Risk model for integrated management system. *Technical Gazette*, 26(6): 1833-1840.

Ali, A., Iqbal, S. & Haider, S.A. 2021. Does governance in information technology matter when it comes to organizational performance in Pakistani public sector organizations? Mediating effect of innovation. *SAGE Open*, 11(2): 1-16.

Ali, M., Man, N., Farrah, M.M. and Omar, S.Z., 2020. Factors influencing behavioral intention of farmers to use ICTs for agricultural risk management in Malaysia. *Pakistan Journal of Agricultural Research*, 33(2), p.295.

Alijoyo, F.A. & Norimarna, S. 2021. The role of enterprise risk management (ERM) using ISO 31000 for the competitiveness of a company that adopts the value chain (VC) model and life cycle cost (LCC) approach: Proceedings of the 3rd International Conference on Business, Management and Finance (ICBMF), Oxford, 11-14 March. Oxford: *International Conference on Business, Management and Finance*.

Anguera, M.T., Blanco-Villaseñor, A. & Losada, J.L. 2018. Revisiting the difference between mixed methods and multimethods: Is it all in the name? *Quality & Quantity*, 52: 2757-2770.

Annamalah, S., Raman, M & Marthandan, G. 2018. Implementation of enterprise risk management (ERM) framework in enhancing business performances in oil and gas sector. *Economies*, *6*(1), 4.

Anton, S.G. & Nucu, A.E.A. 2020. Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management,* 13(11), p. 281.

Arifin, S.R.M. 2018. Ethical considerations in qualitative study. *International Journal of Care Scholars,* 1(2): 30-33.

Azizi, N. & Rowlands, B. 2020. Developing an IT Risk Management Culture Framework. *ICT for an Inclusive World: Industry 4.0–Towards the Smart Enterprise*, 483-491.

Bans-Akutey, A. & Tiimub, B.M. 2021. Triangulation in research. *Academia Letters*, 2.

Benbunan-Fich, R., Desouza, K.C. & Andersen, K.N. 2020. IT-enabled innovation in the public sector: introduction to the special issue. *European Journal of Information Systems*, 29(4): 323-328.

Birkel, H.S., Veile, J.W. & Müller, J.M. 2019. Development of a risk framework for industry 4.0 in the context of sustainability for established manufacturers. *Sustainability,* 11(2): 384.

Blumer, H., 1986. *Symbolic interactionism: Perspective and method*. University of California Press.

Bracci, E., Tallaki, M., Gobbo, G. & Papi, L. 2021. Risk management in the public sector: a structured literature review. *International Journal of Public Sector Management*, 34(2): 205-223.

Braun, V. & Clark, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77-101.

Braun, V., Clarke, V. & Boulton, E. 2021. The online survey as a qualitative research tool. *International Journal of Social Research Methodology,* 24(6): 641-654.

Brocal, F., González-Gaya, C. & Komljenovic, D. 2019. Emerging risk management in industry 4.0: An approach to improve organizational and human performance in the complex systems. *Complexity,* 2: 1-13.

Bryce, C., Chmura, T. & Webb, R. 2019. Internally reporting risk in financial services: An empirical analysis. *Journal of Business Ethics*, 156: 493-512.

Bryman, A. & Bell, E. 2015. *Business research methods*, 4th Edition. New York: Oxford University Press.

Bvuma, S. & Marnewick, C. 2020. An information and communication technology adoption framework for small, medium and micro-enterprises operating in townships South Africa. *The Southern African Journal of Entrepreneurship and Small Business Management*, 12(1): 1-12.

Canedo, E.D., Da Costa, R.P. & de Sousa, R.T. 2018. *Information*, 9(6): 1-17.

Chanopas, A., Krairit, D. & Khang, D.B. 2006. Managing information technology infrastructure: a new flexibility framework. *Management Research News*, 29(10): 632-651.

Clarke, V. & Braun, V. 2013. *Successful Qualitative Research*: A Practical Guide for Beginners. London: SAGE Publications.

Creswell, J.W. 2009. *Research Design*. 3rd edition. United States of America: SAGE Publications.

Creswell, J.W. & Creswell, J.D. 2018. *Research Design.* 5th edition. United states of America: SAGE Publications.

da Silva Etges, A.P.B. & Cortimiglia, M.N. 2019. A systematic review of risk management in innovation-oriented firms*. Journal of Risk Research*, 22(3): 364-381.

de Souza, F.S.R.N., de Avezedo Braga, M.V. & da Cunha, A.S.M. 2020. Incorporation of international risk management standards into federal regulations. *Revista Brasileira de Administração Pública,* 54(1): 59-78.

Dearing, J.W. & Cox, J.G. 2018. Diffusion of innovations theory, principles, and practice. *Health Affairs*, 37(2): 183-190.

Department of Co-operative Governance and Traditional Affairs. 2018. Corporate Governance of Information and Communication Technology policy 2018/19. Mpumalanga: Department of Co-operative Governance & Traditional Affairs.

Department of Forestry, Fisheries and the Environment. 2022. Annual Performance Plan 2022/23. Pretoria: Department of Forestry, Fisheries and the Environment.

Department of National Treasury. 2010. Public sector risk management framework. Department of National Treasury. Available: https://ag.treasury.gov.za/org/rms/rmf/Shared%20Documents/Downloads/00%20Condensed%20Public%20Sector%20Risk%20Management%20Framework.pdf [Accessed: 21 September 2021].

Department of Public Service Administration. 2012. Public service corporate governance of information and communication technology policy framework. Department of Public Service Administration. Available: https://www.gov.za/sites/default/files/gcis_document/201409/cgictpolicyframework.pdf [Accessed: 21 December 2021].

Department of Telecommunications and Postal Services. 2016. The National Integrated ICT policy white paper. Department of Telecommunications and Postal Services. Available:https://www.gov.za/documents/electronic-communications-act-national-integrated-ict-policy-white-paper-3-oct-2016-000. [Accessed: 21 December 2021].

Department of Water and Sanitation. 2021b. *Enterprise-wide Risk Management framework 2020/2021.* Pretoria: Department of Water and Sanitation.

Department of Water and Sanitation. 2021a*. Risk Management Policy 2020/2021*. Pretoria: Department of Water and Sanitation.

Downs, F.S., 1990. Handbook of Research Methodology. *Dimensions of Critical Care Nursing*, *9*(1), p.60.

Drydakis, N., 2022. Artificial Intelligence and Reduced SMEs' Business Risks. A Dynamic Capabilities Analysis During the COVID-19. Pandemic.

ElHaddad, A.A., ElHaddad, N.R. & Alfadhli, M.I. 2020. Internal audit and its role in risk management evidence: The Libyan universities. *International Journal of Academic Research in Business and Social Sciences,* 10(1): 361–377.

Eresia-Eke, C.E. & Soriakumar, A.D. 2021. Strategy implementation barriers and remedies in public sector organisations. *African Journal of Public Affairs,* 12(1): 46-62.

Ettish, A.A., El-Gazzar, S.M. & Jacob, R.A. 2017. Integrating internal control frameworks for effective corporate information technology governance*. Journal of Information Systems and Technology Management,* 14(3):361-370.

European Commission. 2020. *Strategic environmental assessment*. European Commission. Available at: https://environment.ec.europa.eu/law-and-governance /environmental-assessments/strategic-environmental-assessment_en#publications

Everson, M.E.A., Chesley, D.L. & Martens, F.J. 2017. Enterprise risk management: integrating with strategy and performance. Committee of Sponsoring Organizations of the Treadway Commission. Available at https://www.coso.org/Shared%20 Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf [Accessed: 20 June 2020].

Fernandez, V. 2020. *Fundamentals of research methodology*. Barcelona: OmniaScience.

Fourie, W. 2022. Leadership and risk: a review of the literature. *Leadership & Organization Developmental Journal,* 43(4): 550-562.

George, C., 2020. The essence of risk identification in project risk management: an overview. *International Journal of Science and Research (IJSR)*, *9*(2),1553-1557.

Gholami, R., Singh, N. & Agrawal, P. 2021. Information technology/systems adoption in the public sector: Evidence from the Illinois Department of Transportation. *Journal of Global Information Management*, 29(4): 172-194.

Goundar, S. 2012. *Research Methodology and Research Method.* Victoria University of Wellington.

Gunawan, J. 2015. Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, 1(1): 10-11.

Haines, G. 2017. Ethical considerations in qualitative case study research recruiting participants with profound intellectual disabilities. *Research Ethics,* 13(3-4): 219-232.

Hakim, A.L., Faizah, E.N. & Mas'adah, N. 2021. Analysis of leadership style by using the model of Hersey and Blanchard. *Journal of Leadership in Organizations*, 3(2): 138-148.

Hammarberg, K., Kirkman, M. & de Lacey, S. 2016. Qualitative research methods: when to use them and how to judge them. *Human reproduction*, *31*(3): 498-501.

Hayashi Jr, P., Abib, G. & Hoppen, N. 2019. Validity in qualitative research: A processual approach. *The Qualitative Report*, *24*(1), 98-112.

Hussain, O.K., 2022. The process of risk management needs to evolve with the changing technology in the digital world. *Service Oriented Computing and Applications*,*16*(3), pp.143-145.

Information Systems Audit and Control Association (ISACA). 2019. COBIT 2019 and risk management. (April).

Information Technology Authority. 2017. *IT risk management framework*. Information Technology Authority. Available at: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf

Institute of International Finance and McKinsey & Company. 2017. The future of risk management in the digital era. Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx [Accessed: 14 June 2021].

Iorga, M. & Karmel, A. 2016. Chapter 7: Managing risk in the cloud. In Vacca, J.R. (Ed.). *Cloud computing security: Foundations and challenges*. Boca Raton: CRC Press, 95-114.

Jansen, H. 2010. The logic of qualitative survey research and its position in the field of social research methods. Forum: *Qualitative Social Research,* 11(2).

Joel, C. & Vyas-Doorgapersad, S. 2019. An analysis of risk management within the Department of Trade and Industry. *Journal of Contemporary Management*, *16*(1), 357-375.

Kabir, S.M.S. 2016. *Basic guidelines for research: An introductory approach for all disciplines*. Chittagong: Book Zone Publication.

Kanu, M.S., 2020. Integrating enterprise risk management with strategic planning for improved firm performance. *European Journal of Business & Management Research*, 5(5): 1-11.

Kassa, S.G. & CISA, C. 2017. IT asset valuation, risk assessment and control implementation model. *ISACA Journal*, *3*(1), 1-9.

Khan, F.N. & Majeed, M.T. 2020. ICT and e-government as the sources of economic growth in information age: Empirical evidence from South Asian economies. *A Research Journal of South Asian Studies*, 34(1): 227-249.

Kim, S. & Kim, D. 2020. ICT implementation and its effect on public organisations: The case of digital customs and risk management in Korea. *Sustainability*, 12(8): 1-19.

Kitsios, F., Chatzidimitriou, E. & Kamariotou, M. 2022. Developing a risk analysis strategy framework for impact assessment in information security management systems. *Sustainability,* 14(3): 1-19.

Kivunja, C. & Kuyini, A.B. 2017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education,* 6(5): 26-41.

Kong, Y., Lartey, P.Y. & Bah, F.B.M. 2018. The value of public sector risk management: An empirical assessment of Ghana. *Administrative Sciences*, *8*(3), 1-18

Korstjens, I. & Moser, A. 2017. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice,* 24(1): 120-124.

KPMG International, K. n.d. Modernizing government : Global trends.

Künzli, A. & Gile, D. 2021. The impact of ICTs on surveys and interviews in translation and interpreting studies. *Parallèles,* 33(2): 1-17.

Kuzminykh, I., Ghita, B., Sokolov, V. and Bakhshi, T. Information security risk assessment. *Encyclopedia*, 1(3): 602-617.

Labra, O. Castro, C. & Wright, R. 2022. Thematic analysis in social work: A case study. In Nikku, B.R. (Ed.). *Global social work: Cutting edge issues and critical reflections.* London: IntechOpen, 183-202.

Larasati, D.A., Ratri, M.C., & Nasih, M. 2019. Independent audit committee, risk management committee, and audit fees. *Cogent Business & Management,* 6(1): 1-15.

Lawani, A. 2021. Critical realism: what you should know and how to apply it*. Qualitative Research Journal*, 21(3): 320-333.

Ludwig, L. & Mattedi, M. A. 2018. The Information and Communication Technologies in the risk management of social and environmental disasters. *Ambiente and Sociedade*, 21: 1-22.

Mahama, H., Elbashir, M. & Sutton, S. 2022. Enabling enterprise risk management maturity in public sector organisations. *Public Money & Management*, 42(6): 403-407.

Mardiana, S. 2020. Modifying research onion for information systems research. *Solid State Technology*, 63(4): 1202-1210.

Marks, L. 2019. The optimal risk management framework: Identifying the requirements and selecting the framework. *ISACA Journal*, 1(): 40-45.

Martens, F.J. & Rittenberg, L. 2020. Risk appetite – critical to success*. Committee of Sponsoring Organizations of the Treadway Commission.* Available at: https://www.coso.org/Shared%20Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf [Accessed: 23 June 2021].

Maruhun, E.N.S., Atan, R. & Yusuf, S.N.S. 2021. Value creation of enterprise risk management: Evidence from Malaysian Shariah-compliant firms. I*nternational Journal of Academic Research in Business & Social Sciences*, 11(10): 922-938.

Mauthner, N.S., 2020. Chapter 12: Research philosophies and why they matter. In Townsend, K., Saunders, M.N.K. & Loudoun, R. (Eds.). *How to Keep your Doctorate on Track*. Northampton: Edward Edgar Publishing, 76-86.

Maxwell, J.A., 2018. Collecting qualitative data: A realist approach. In Flick, U. (Ed.). *The SAGE handbook of qualitative data collection.* London: SAGE Publications Limited, 19-32.

Mazhar, S.A., Anjum, R., Anwar, A.I. & Khan, A.A. 2021. Methods of data collection: a fundamental tool of research. *Journal of Integrated Community Health,* 10(1): 6-10.

Mazumder, M.M.M. & Hossain, D.M. 2018. Research on corporate risk reporting: Current trends and future avenues. *The Journal of Asian Finance, Economics and Business*, 5(1): 29-41.

Melnikovas, A. 2018. Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of Futures Studies,* 23(2): 29-44.

Mensah, R.O., Frimpong, F. & Acquah, A. 2020. Discourses on conceptual and theoretical frameworks in research: Meaning and implications for researchers. *Journal of African Interdisciplinary Studies*, 4(5): 53-64.

Meşe, E. & Çiğdem, S. 2021. Factors influencing EFL students' motivation in online learning: A qualitative case study. *Journal of Educational Technology and Online Learning,* 4(11): 11-22.

Mishchenko, S., Naumenkova, S. & Mishchenko, V. 2021. Innovation risk management in financial institutions. *Investment Management and Financial Innovations*, 18(1):191-203.

Mitchell, A. and Education, A.E., 2018. A review of mixed methods, pragmatism and abduction techniques. In *Proceedings of the European Conference on Research Methods for Business & Management Studies* (pp. 269-277).

Mkhize, P., Mtsweni, E.S. and Buthelezi, P., 2016. Diffusion of innovations approach to the evaluation of learning management system usage in an open distance learning institution. *International Review of Research in Open and Distributed Learning*, *17*(3), pp.295-312.

Mkhize, T. R. & Davids, M.N. 2021.Towards a digital resource mobilisation approach for digital inclusion during covid-19 and beyond: A case of a township school in south africa1', *Educational Research for Social Change*, 10(2): 18–32.

Mohammad, S.M. 2020. *Risk management in information technology* Available at: https://dx.doi.org/10.2139/ssrn.3625242

Nadikattu, R.R. 2019. Risk management in private sector. *International Journal of Computer Trends and Technology*, 67(5): 202-207.

Naidoo, I.P. & Hoque, M. 2018. Impact of information technology on innovation in determining firm performance. *African Journal of Science, Technology, Innovation and Development,* 10(6): 643-653.

Nakano, D. & Muniz, J. 2018. Writing the literature review for empirical papers. *Production*, 28: 1-9.

Nalubega, T. & Uwizeyimana, D.E. 2019. Public sector monitoring and evaluation in the Fourth Industrial Revolution: Implications for Africa. *Africa's Public Service Delivery and Performance Review*, *7*(1): 1-12.

National Institute of Standards and Technology. 2018. Risk management framework for information systems and organizations. National Institute of Standards and Technology. Available: https://www.itdojo.com/oolruchu/2019/01/NIST_SP_800-37r2.pdf [Accessed: 23 June 2021].

National Institute of Standards and Technology. 2020. Integrating cybersecurity and enterprise risk management (ERM). 8286. National Institute of Standards and Technology. Available:https://complexdiscovery.com/wp-content/uploads/2020/03/NIST.IR_.8286.pdf [Accessed: 20 June 2021].

Nazir, M.A. & Khan, R.S. 2022. The impact and factors affecting information and communication technology adoption in small and medium-sized enterprises: A perspective from Pakistan. *Journal of Organisational Studies and Innovation*, 9(1): 20-46.

Nel, D. 2019. Risk management in the South African local government and its impact on service delivery*. International Journal of Management Practice,* 12(1): 60-80.

Ngulube, P. 2020. The Movement of Mixed Methods Research and the Role of Information Science Professionals. *Angewandte Chemie International Edition,* 6(11): 951–952. [Preprint].

Nhan, N.T. 2020. *The role of theoretical framework and methods in research*. OSF Preprints: 1-4.

Nilmanat, K. & Kurniawan, T. 2020. The Quest in Case Study Research. Pacific Rim *International Journal of Nursing Research,* 25(1): 1-6.

Noble, H. & Heale, R. 2019. Triangulation in research, with examples. *Evidence-Based Nursing*, 22(3): 67-68.

Noronha, M.M. & Pamnani, D.S. 2021. A study of association between economic value added and net operating profit after tax: a case study of Divis Laboratories and Lupin Limited. *EPRA International Journal of Economics, Business and Management Studies*, 8(6): 8-14.

Oben, A.I. 2021. Research instruments: A questionnaire and an interview guide used to investigate the implementation of higher education objectives and the attainment of Cameroon’s vision 2035. *European Journal of Education Studies*, 8(7): 113-130.

Oshagbemi, T. 2017. *Leadership and management in universities: Britain and Nigeria. Berlin*: De Gruyter. Available at: https://scholar.google.co.za/scholar?q=Oshagbemi,+T.+2017.+Leadership+and+management+in+universities+:+Britain+and+Nigeria.+Berlin:+De+Gruyter.&hl=en&as_sdt=0&as_vis=1&oi=scholart [Accessed: 19 December 2021].

Park, Y.S., Konge, L. & Artino, A.R. 2020. The positivism paradigm of research*. Academic Medicine,* 95(5): 690-694.

Park, M. & Singh, N.P., 2023. Predicting supply chain risks through big data analytics: role of risk alert tool in mitigating business disruption. *Benchmarking: An International Journal*, 30(5), pp.1457-1484.

Patel, M. & Patel, N. 2019. Exploring research methodology: Review article. *International Journal of Research & Review,* 6(3): 48-55.

Patiño, S., Solís, E.F., Yoo, S.G. and Arroyo, R. 2018. ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005. In *2018 International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 75-82). IEEE.

Polit, D.F. & Beck, C.T. 2017*. Nursing research: Generating and Assessing Evidence for Nursing Practice.* 10th edition. Philadelphia: Wolters Kluwer Health.

Qammaz, A.S. & AlMaian, R.Y. 2018. The role of information and communication technology in construction risk management. *Proceedings of the International Conference on Industrial Engineering and Operations Management,* Bandung, 6-8 March. Bandung: IEOM Society International.

Rachmawati, R., Choirunnisa, U. & Pambagyo, Z.A. 2021. Work from home and the use of ICT during the COVID-19 pandemic in Indonesia and its impact on cities in the future. *Sustainability*, 13(12): 1-17.

Rashid, Y., Rahid, A. & Warraich, M.A. 2019. Case study method: A step-by-step guide for business researchers. *International Journal of Qualitative Methods*, 18: 1-13.

Ratheeswari, K. 2018. Information communication technology in education. *Journal of Applied and Advanced research*, *3*(1): 45-47.

Robinson, O.C. 2022. Conducting thematic analysis on brief texts: The structured tabular approach. *Qualitative Psychology*, 9(2): 194-208.

Rogers, E.M., 1995. Diffusion of Innovations: modifications of a model for telecommunications. *Die diffusion von innovationen in der telekommunikation*, pp.25-38.

Roller, M.R. 2019. A quality approach to qualitative content analysis: Similarities and differences compared to other qualitative methods. Forum: *Qualitative Social Research,* 20(3).

Rugg, D. n.d. An Introduction to Triangulation. UNAIDS Monitoring and Evaluation Fundamentals. Available at: http://www.unaids.org/en/media/unaids/contentassets/documents/document/2010/10_4-Intro-to-triangulation-MEF.pdf. [Accessed: 14 January 2023].

Ryan, G. 2018. Introduction to positivism, interpretivism and critical theory. *Nurse Researcher,* 25(4): 41-49.

Saeidi, P., Saeidi, S.P. & Gutierrez L. 2021. The influence of enterprise risk management on firm performance with the moderating effect of intellectual capital dimensions. *Economic Research-Ekonomska Istraživanja*, 34(1): 122-151.

Salisu, Y. & Bakar, L.J.A. 2020. Technological capability, relational capability and firms' performance: The role of learning capability. *Revista de Gestão,* 27(1): 79-99.

Saunders, M.N.K., Lewis, P. & Thornhill, A. 2019. *Research methods for business students*. 8th edition. New York: Pearson Education.

Schandl, A. & Foster, P.L. 2019. COSO internal control – integrated framework: An implementation guide for the healthcare provider industry. Committee of Sponsoring

Organizations of the Treadway Commission. Available at: https://www.coso.org/Shared%20Documents/CROWE-COSO-Internal-Control-Integrated-Framework.pdf [Accessed: 19 December 2021].

Schutte, B. & Marx, B. 2018. The role of information technology in the risk management of businesses in South Africa. *Journal for New Generation Sciences*,16(2): 92-111.

Shabbir, M.Q. & Gardezi, S.B.W., 2020. Application of big data analytics and organizational performance: the mediating role of knowledge management practices. *Journal of Big Data*, 7(1), pp.1-17.

Shaikh, S. & Shaikh, R. 2019. Modelling of dynamic/situational leadership for effective entrepreneurship development. *Journal of Model Based Research*, 1(1): 1-6.

Shand, R., Parker, S. & Liddle, J. 2022. After the applause: Understanding public management and public service ethos in the fight against Covid-19. *Public Management Review*: 1-23.

Sharma, B. 2018. Processing of data analysis. *Biostatistics and Epidemiology International Journal, 1*(1): 3-5.

Shava, E. & Vyas-Doorgapersad. 2021. Information communication technology (ICT) and smart service delivery in the fourth industrial revolution: A case of the city of Johannesburg. *Journal of Public Administration*, 56(4.1): 986–1001.

Shedden, P., Ahmad, A. & Smith, W. 2016. Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems*, 39(1): 15.

Shipalana, M.L. 2020. Innovative management in the public service: Towards service delivery imperatives: Proceedings from the 5th Annual International Conference on Public Administration and Development Alternatives. Virtual, 7-9 October. Virtual conference: IPADA.

Srinivas, K., 2019. Process of risk management. In *Perspectives on Risk, Assessment and Management Paradigms*. IntechOpen.

Taylor, R.G. 2015. Potential problems with information security risk assessments. *Information Security Journal: A Global Perspective*, 24(4-6): 177-184.

Teymouri, M. & Ashoori, M. 2011. The impact of information technology on risk management. *Procedia Computer Science*,*3*, 1602-1608.

Institute of Risk Management South Africa. 2016. IRMSA Risk Report: South Africa Risks 2016. IRMSA. Available at: https://cdn.ymaws.com/www.irmsa.org.za/resource/resmgr/2016_risk_report/irmsa_2016_risk_report.pdf

Institute of Risk Management South Africa. 2018. IRMSA Risk Report: South Africa Risks 2016. IRMSA. Available at: https://www.irmsa.org.za/page/IRMSARiskReport [Accessed: 19 December 2021].

Thompson, G. & Glasø, L. 2018. Situational leadership theory: a test from a leader-follower congruence approach. *Leadership & Organization Development Journal*, 39(5): 574-591.

Tlhogane, E.M., Miruka, C.O. & Gumede, N., 2018. Implementing healthcare governance structures in a decentralised system in the Northwest Province of South Africa. *Journal of Public Administration*, 53(1), pp.64-73.

Torrentira, M.C. 2020. Online data collection as adaptation in conducting quantitative and qualitative research during the Covid-19 pandemic. *European Journal of Education Studies*, 7(11): 78-87.

Tremblay, S., Castiglione, S. & Audet, L. 2021. Conducting qualitative research to respond to Covid-19 challenges: Reflections for the present and beyond. *International Journal of Qualitative Methods, 2*0: 1-8.

Tupa, J. & Simota, J. 2017. Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing*, 11: 1223-1230.

Tworek, P. 2016. Risk Management in the Public Sector Organisations-Principles, Methods and Tools. In *8th International Scientific Conference on Managing and Modelling of Financial Risks* (pp. 1022-1029).

Uctu, R. & Essop, H. 2020. Identifying the strength and weaknesses of the South African tech-based industries: Insights from the Swiss South African business development programme. *African Journal of Science, Technology, Innovation and Development*, *12*(4), 517-528.

Usman, S.H., 2019. MIT Governance implementation in enterprise: A review. *International Journal of Research in Electronics and Computer Engineering*, 7(2), pp.3129-3134.

Van Dongen, N. & Sikorski, M. 2021. Objectivity for the research worker. *European Journal for Philosophy of Science*, 11(93): 1-25.

Varpio, L., Paradis, E. & Uijtdehaage, S. 2020. The distinctions between theory, theoretical framework, and conceptual framework. *Academic Medicine,* 95(7): 989-994.

Weeserik, P. B. & Spruit, M. 2018. Improving operational risk management using business performance management technologies. *Sustainability,* 10(3), 640.

Western Cape Government. 2013. Strategic ICT planning framework. Provincial Government of the Western Cape. Available: https://www.dpsa.gov.za/dpsa2g/documents/psictm/2014/ICT%20Planning%20Framework.pdf [Accessed: 21 September 2021].

Yue, X., Shao, X. & Li, R.Y.M. 2020. Risk prediction and assessment: Duration, infections, and death toll of the Covid-19 and its impact on China's economy*. Journal of Risk Financial Management*, 13(4): 1-26.

Zahle, J. 2021. Objective data sets in qualitative research. *Synthese,* 199 (1-2): 101-117.

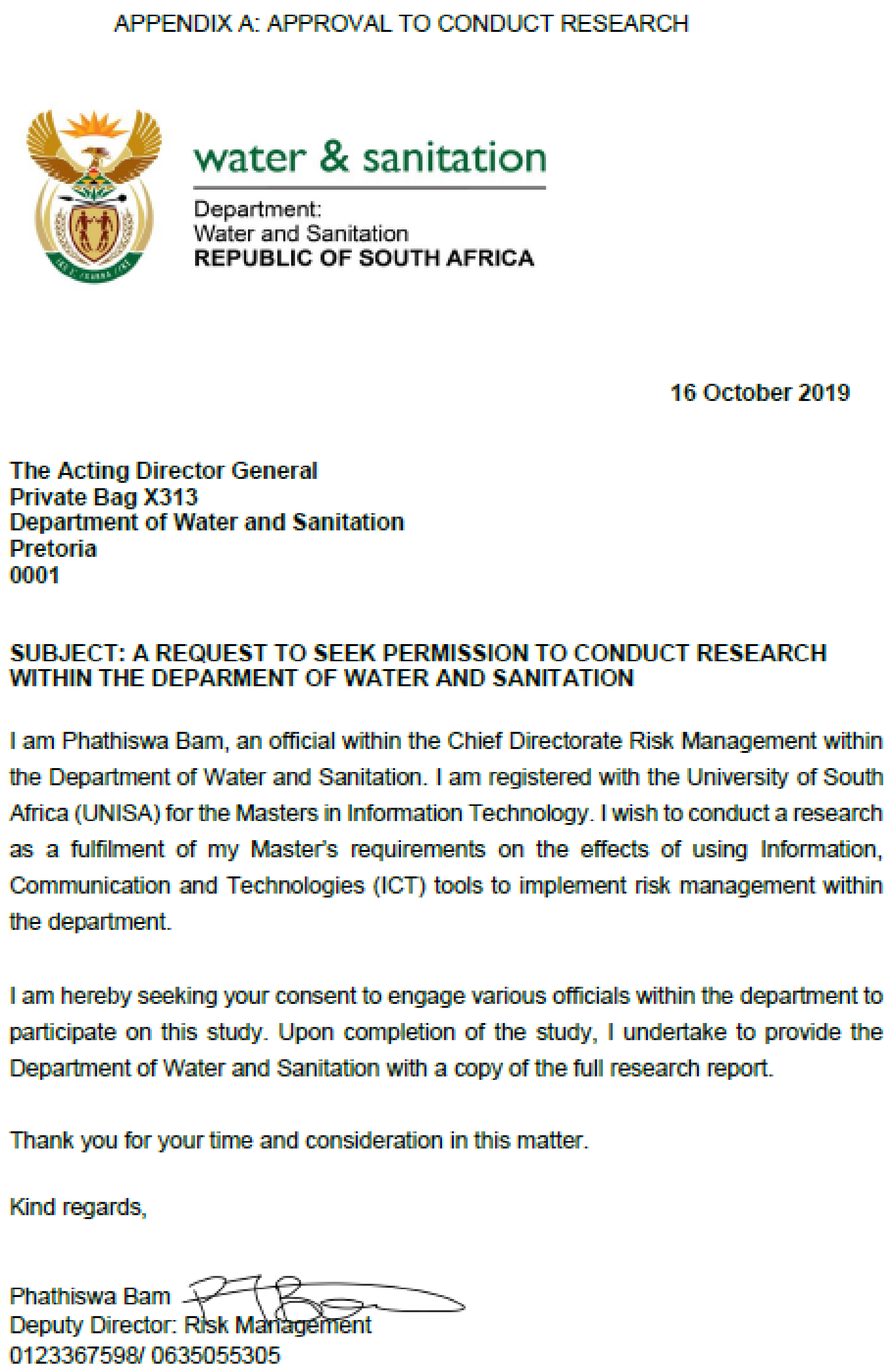
Zainudin, Z., Samad, S.A. & Altounjy, R. 2019. The determinants factors of an effective risk-aware culture of firms in implementing and maintaining risk management program. *International Journal of Financial Research*, 11(5): 459-465.

Zanfei, A. & Seri, P. 2016. The role of ICT, skills and organizational change in public sector performance. *Argomenti*, (3), 5-30.

Zhong, Y., Li, Y. & Ding, J. 2021. Risk management: Exploring emerging human resource issues during the Covid-19 pandemic. *Journal of Financial Research,* 14(5): 1-23.

APPENDICES

Appendix A: Request approval to conduct research



APPENDIX A: APPROVAL TO CONDUCT RESEARCH

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

16 October 2019

The Acting Director General
Private Bag X313
Department of Water and Sanitation
Pretoria
0001

SUBJECT: A REQUEST TO SEEK PERMISSION TO CONDUCT RESEARCH WITHIN THE DEPARMENT OF WATER AND SANITATION

I am Phathiswa Bam, an official within the Chief Directorate Risk Management within the Department of Water and Sanitation. I am registered with the University of South Africa (UNISA) for the Masters in Information Technology. I wish to conduct a research as a fulfilment of my Master's requirements on the effects of using Information, Communication and Technologies (ICT) tools to implement risk management within the department.

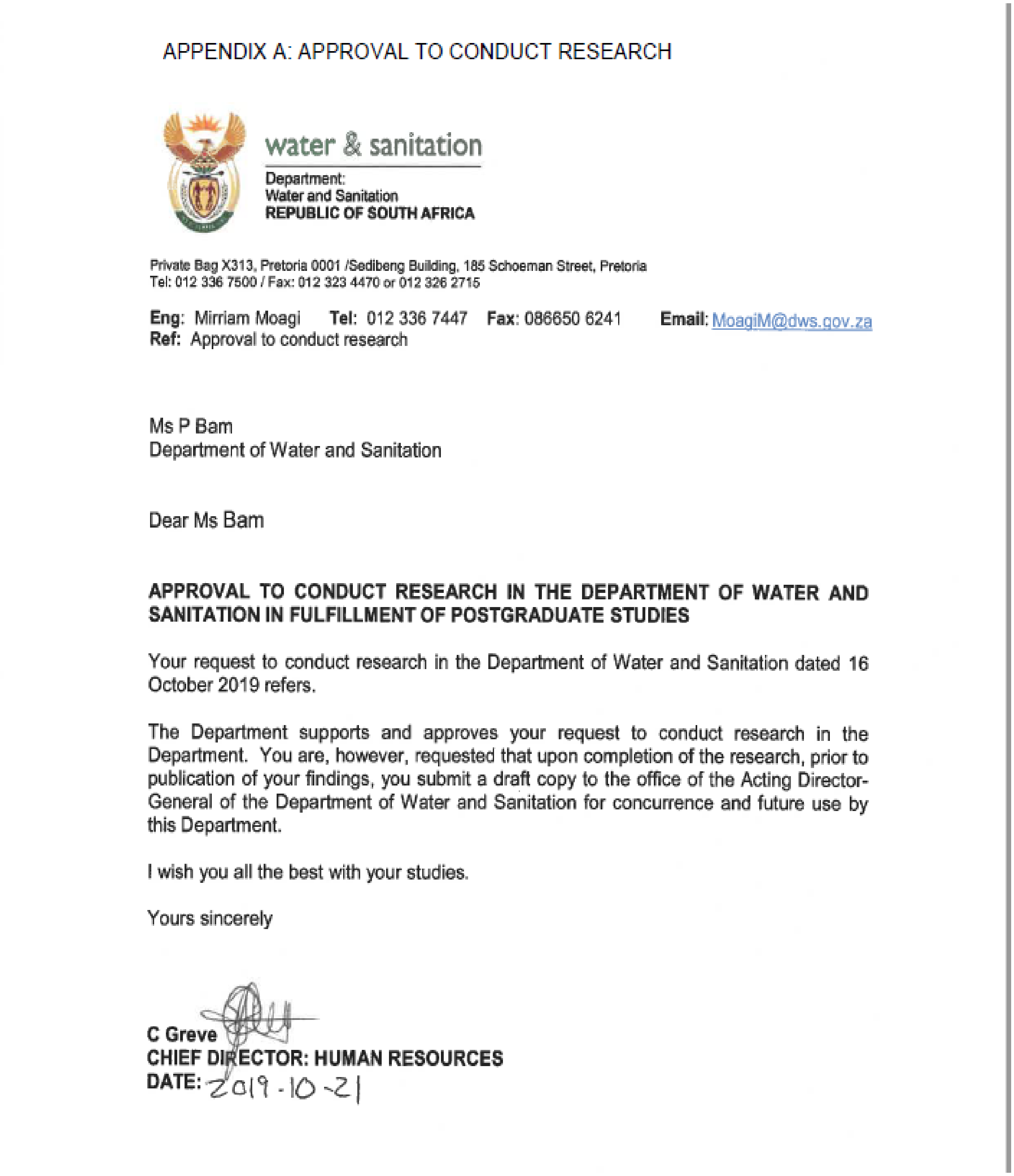
I am hereby seeking your consent to engage various officials within the department to participate on this study. Upon completion of the study, I undertake to provide the Department of Water and Sanitation with a copy of the full research report.

Thank you for your time and consideration in this matter.

Kind regards,

Phathiswa Bam
Deputy Director: Risk Management
0123367598/ 0635055305

Appendix B: Approval to conduct research in the Department of Water and Sanitation granted



APPENDIX A: APPROVAL TO CONDUCT RESEARCH

water & sanitation

Department:
Water and Sanitation
REPUBLIC OF SOUTH AFRICA

Private Bag X313, Pretoria 0001 /Sedibeng Building, 185 Schoeman Street, Pretoria
Tel: 012 336 7500 / Fax: 012 323 4470 or 012 326 2715

Enq: Mirriam Moagi **Tel:** 012 336 7447 **Fax:** 086650 6241 **Email:** MoagiM@dws.gov.za
Ref: Approval to conduct research

Ms P Bam
Department of Water and Sanitation

Dear Ms Bam

APPROVAL TO CONDUCT RESEARCH IN THE DEPARTMENT OF WATER AND SANITATION IN FULFILLMENT OF POSTGRADUATE STUDIES

Your request to conduct research in the Department of Water and Sanitation dated 16 October 2019 refers.

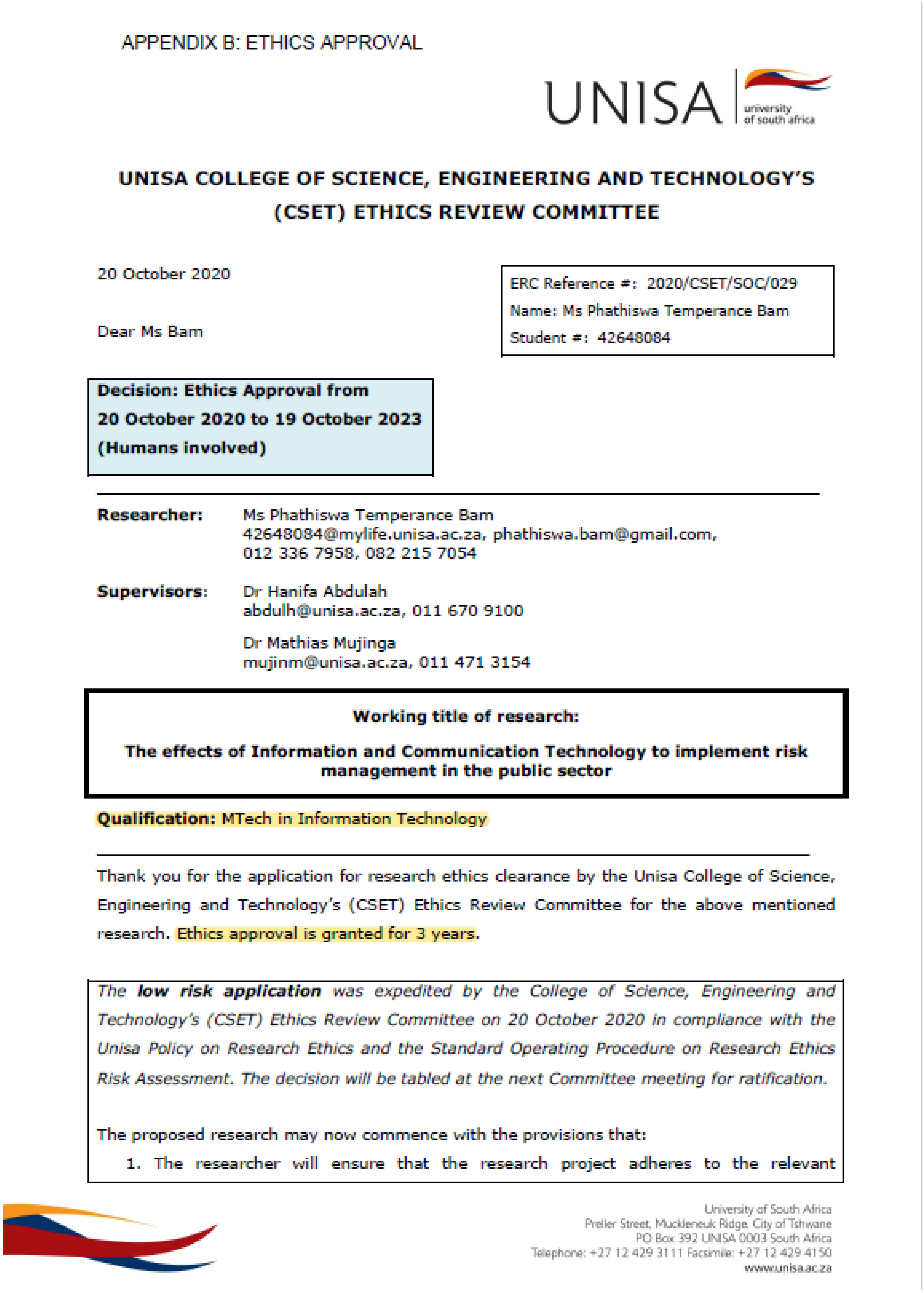
The Department supports and approves your request to conduct research in the Department. You are, however, requested that upon completion of the research, prior to publication of your findings, you submit a draft copy to the office of the Acting Director-General of the Department of Water and Sanitation for concurrence and future use by this Department.

I wish you all the best with your studies.

Yours sincerely

C Greve
CHIEF DIRECTOR: HUMAN RESOURCES
DATE: 2019-10-21

Appendix C: Ethics approval



APPENDIX B: ETHICS APPROVAL

UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

20 October 2020

ERC Reference #: 2020/CSET/SOC/029
Name: Ms Phathiswa Temperance Bam
Student #: 42648084

Dear Ms Bam

Decision: Ethics Approval from 20 October 2020 to 19 October 2023 (Humans involved)

Researcher: Ms Phathiswa Temperance Bam
42648084@mylife.unisa.ac.za, phathiswa.bam@gmail.com,
012 336 7958, 082 215 7054

Supervisors: Dr Hanifa Abdulah
abdulh@unisa.ac.za, 011 670 9100

Dr Mathias Mujinga
mujinm@unisa.ac.za, 011 471 3154

Working title of research:

The effects of Information and Communication Technology to implement risk management in the public sector

Qualification: MTech in Information Technology

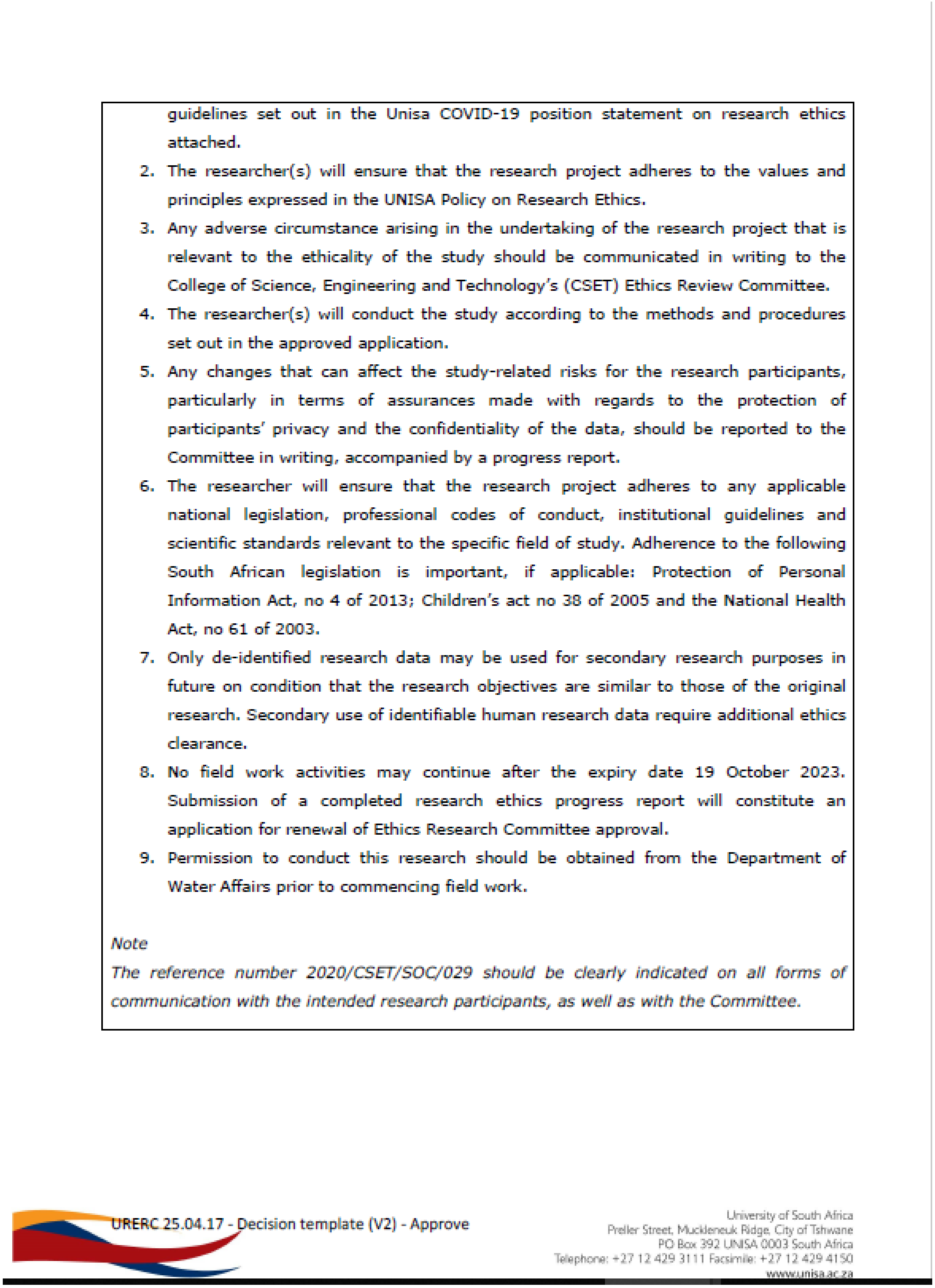
Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **low risk application** was expedited by the College of Science, Engineering and Technology's (CSET) Ethics Review Committee on 20 October 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

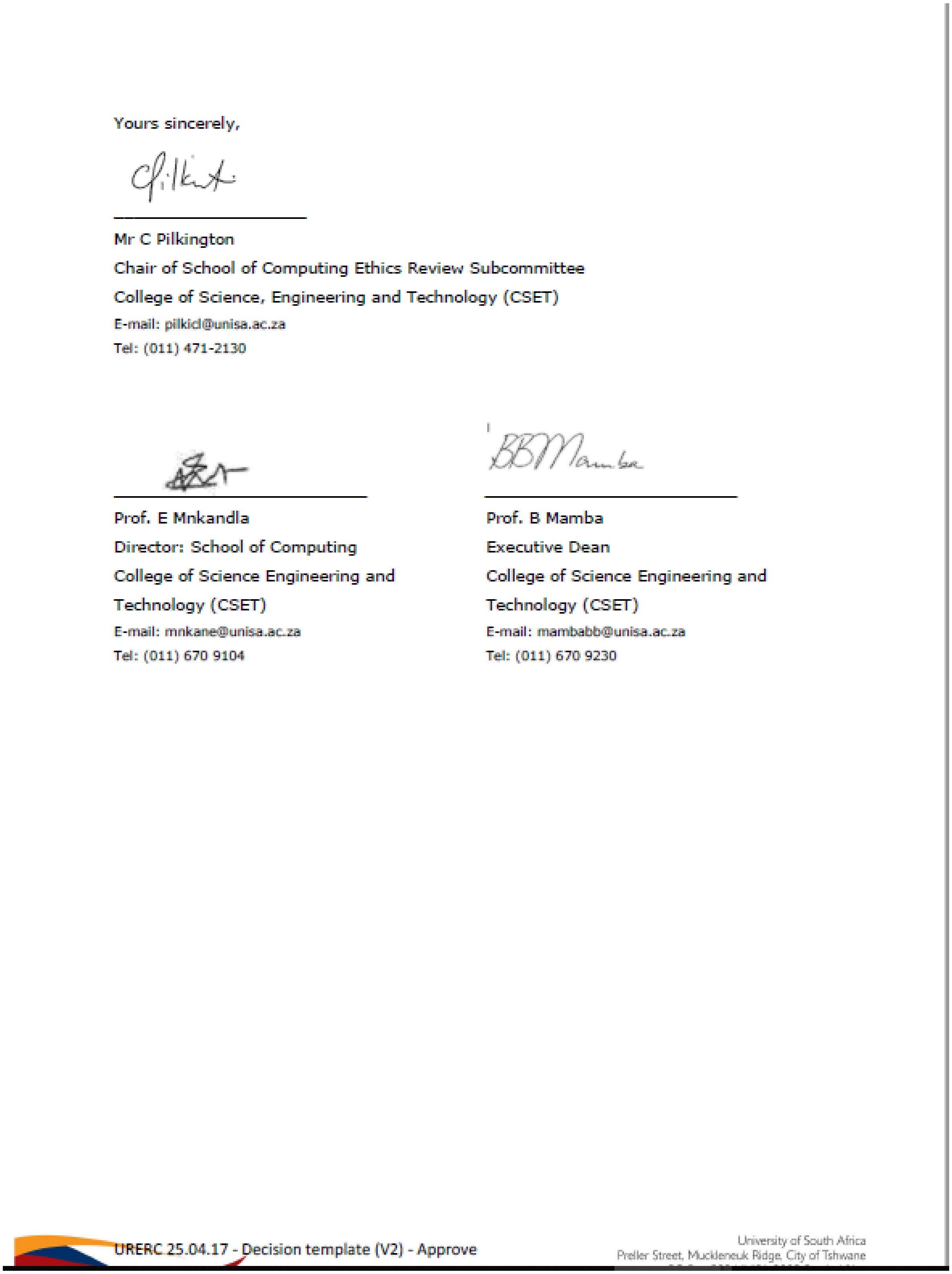


guidelines set out in the Unisa COVID-19 position statement on research ethics attached.

2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology's (CSET) Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date 19 October 2023. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.
9. Permission to conduct this research should be obtained from the Department of Water Affairs prior to commencing field work.

Note

The reference number 2020/CSET/SOC/029 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.



Yours sincerely,

Mr C Pilkington
Chair of School of Computing Ethics Review Subcommittee
College of Science, Engineering and Technology (CSET)
E-mail: pilkicl@unisa.ac.za
Tel: (011) 471-2130

Prof. E Mnkandla
Director: School of Computing
College of Science Engineering and
Technology (CSET)
E-mail: mnkane@unisa.ac.za
Tel: (011) 670 9104

BBMamba

Prof. B Mamba
Executive Dean
College of Science Engineering and
Technology (CSET)
E-mail: mambabb@unisa.ac.za
Tel: (011) 670 9230

Appendix D: Request for participants

Ethics clearance reference number: 2020/CSET/SOC/029

23 October 2020

Title: The effects of information and communication technology (ICT) to implement risk management in the public sector

Dear Prospective Participant

My name is Phathiswa Bam, and I am doing research with Dr H Abdullah, a Senior Lecturer in the Department of Information System, School of Computing towards a MTech in Information Technology at the University of South Africa. We are inviting you to participate in a study entitled the effects of information and communication technology (ICT) to implement risk management in the public sector.

WHAT IS THE PURPOSE OF THE STUDY?

The main purpose of this study is to investigate the use of ICT to support the implementation of risk management activities in the public sector. This study intends to determine if the use of ICT plays any role on the effectiveness of risk management.

WHY AM I BEING INVITED TO PARTICIPATE?

You were selected to participate in this survey because you are currently involved in the risk management activities within the department to ensure effective implementation and creating a risk culture. The key role you play as a risk practitioner, risk owner and risk champion including the IT support you are providing to the risk management team will play a critical role in this study.

I have been granted permission to conduct this study by the Human Resources Development unit in the Department of Water and Sanitation where I am also an employee. As an employee of the department and a risk practitioner within the Chief Directorate Risk Management, I have access to the participants' contact details. In my capacity, I work with the selected participants on a daily basis.

There are a number of 40 participants selected to take part in this study and they are located in head office, regional offices in all nine provinces and cluster offices.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves interviews and a survey through a questionnaire. The interviews will be conducted telephonically and will be audio taped. The survey will be done anonymously through an online questionnaire. The questions that will be asked are around the availability and accessibility to ICT resources, the use of those resources as well as how the participants use these resources to support risk management implementation. The interviews may not take more than an hour and follow up interviews may be done in cases where further clarity is required. The online survey will take approximately not more than 30 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

The participants who are involved in risk management activities in the department will be requested to voluntarily participate. As this is voluntary and there is no compensation of any form, the participants can withdraw from the study when they are no longer interested.

If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

The participants may be inconvenienced in terms of the time they may be required to take away from their planned work schedule to participate on this research.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

To ensure confidentiality, pseudonyms will be allocated to the interview participants. The online questionnaire will remain anonymous.

For the interviews, the names of the participants will be replaced by pseudo names to ensure that the privacy of the participants is maintained. During the interviews, the name of the participants will not be recorded.

The participants' answers will be given a code number, or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings*.* The fact that the researcher is part of the department, and the process will not put the participant under any compromised position.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet in the researcher's capacity. *F*or future research or academic purposes, electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. After 5 years, the records of the interviews and the surveys will be deleted from the hard drive of the researcher's computer.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing [*and Research Permission Subcommittee of the Senate Research and Innovation and Higher Degrees Committee (RPSC) if applicable*]*,* Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

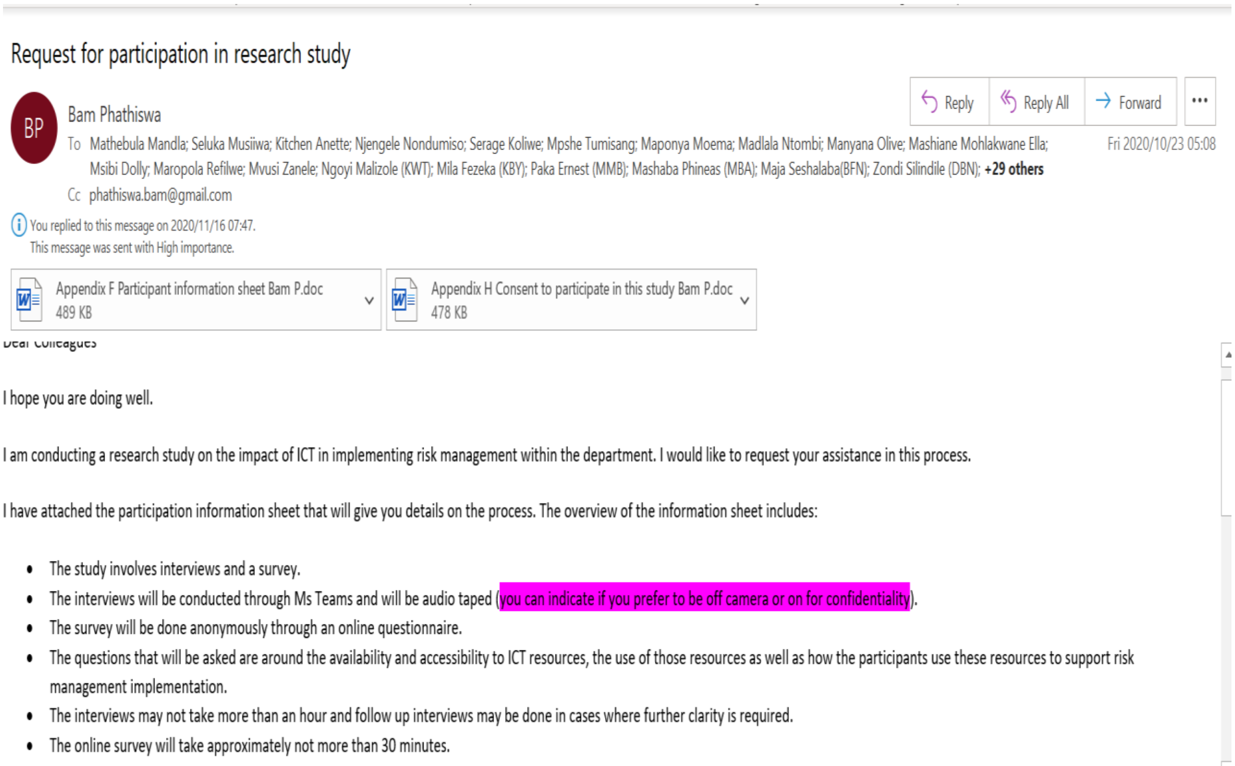
HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

The summary of the outcomes of this study can be made available for the participants. If you would like to be informed of the final research findings, please contact Phathiswa Bam on 0822157054 or phathiswa.bam@gmail.com. The summary of the findings is accessible for two years. Please do not use home telephone numbers. Departmental and/or mobile phone numbers are acceptable. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Phathiswa at 0822157054 or phathiswa.bam@gmail.com

Should you have concerns about the way in which the research has been conducted, you may contact Dr H Abdullah at 011 670 9100, email address abdulh@unisa.ac.za. Contact the research ethics chairperson of the UNISA's Ethics Research Committee, 011 670 9105 or SocEthics@unisa.ac.za if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study. Thank you.

Signed:
Phathiswa Bam



Request for participation in research study

Bam Phathiswa
To Mathebula Mandla; Seluka Musiiwa; Kitchen Anette; Njengele Nondumiso; Serage Koliwe; Mpshe Tumisang; Maponya Moema; Madlala Ntombi; Manyana Olive; Mashiane Mohlakwane Ella; Msibi Dolly; Maropola Refilwe; Mvusi Zanele; Ngoyi Malizole (KWT); Mila Fezeka (KBY); Paka Ernest (MMB); Mashaba Phineas (MBA); Maja Seshalaba(BFN); Zondi Silindile (DBN); **+29 others**
Fri 2020/10/23 05:08
Cc phathiswa.bam@gmail.com

You replied to this message on 2020/11/16 07:47.
This message was sent with High importance.

Appendix F Participant information sheet Bam P.doc
489 KB

Appendix H Consent to participate in this study Bam P.doc
478 KB

Dear Colleagues

I hope you are doing well.

I am conducting a research study on the impact of ICT in implementing risk management within the department. I would like to request your assistance in this process.

I have attached the participation information sheet that will give you details on the process. The overview of the information sheet includes:

- The study involves interviews and a survey.
- The interviews will be conducted through Ms Teams and will be audio taped (you can indicate if you prefer to be off camera or on for confidentiality).
- The survey will be done anonymously through an online questionnaire.
- The questions that will be asked are around the availability and accessibility to ICT resources, the use of those resources as well as how the participants use these resources to support risk management implementation.
- The interviews may not take more than an hour and follow up interviews may be done in cases where further clarity is required.
- The online survey will take approximately not more than 30 minutes.

Appendix E: Consent form for the participants

CONSENT TO PARTICIPATE IN THIS STUDY

I, __________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the interview through Ms Teams.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname………………………………………… (please print)

Participant Signature…………………………………………… .Date…………………

Researcher's Name & Surname……………………………………… (please print)

Researcher's signature………………………………………….. Date…………………

Appendix F: Questionnaire

BACKGROUND

I am conducting a research on above the subject towards fulfilling my MTech in Information Technology at UNISA. The intention of this questionnaire is to determine whether integrating technology when implementing day to day risk management activities has an impact on risk management effectiveness. To collect accurate and relevant data, I would like to ask you to participate in this study by responding to the questions below. For confidentiality, the questionnaire will be done only to ensure anonymity. The responses will be sent online to ensure anonymity. Please note that the information provided will only be used for the purpose of the study and will be treated with confidentiality.

INSTRUCTIONS

This questionnaire is divided into the following categories:

Section 1: General Information about the respondent and their professional experience
Section 2: Access and Use of Information Communication Technology (ICTs) in risk management
Section 3: Attitudes of the user towards using ICT in risk management
Section 4: Challenges experienced by the users in using ICT

Section 1: General Information about the respondent and their professional experience

Instruction: Mark with an X next to an appropriate answer

- Please indicate the name of your business unit, cluster, or regional office.
  ____
  ____
  ____
  ____

- Please indicate your age.

  Between 25 – 35 · Between 36 – 46 · Between 47 – 60 ·

- What role do you play in risk management?

  Risk Owner · Risk Champion · Risk Practitioner · IT Official ·

4. What is your position?

Chief Director · Director · Deputy Director · Assistant Director ·

Risk Practitioner · Administrator · Other ·

5. What is your highest level of qualifications?

Matric · Certificate · Diploma · Degree · Masters · PHD ·

Other ·

Section 2: Access and use of Information Communication Technology (ICT) in risk management

2.1 Access to ICT resources

A. Do you have the following ICT equipment? Please select the ones you currently have.

Equipment	Yes
Desktop	.
Laptop	.
Smartphone	.

Tablet	.

B. Do you have access to the following? Please select the ones you are currently have.

Resource	Yes
Network drive	.
IT System (SAP GRC)	.
Internet explorer	.
Email	.
Ms Teams	.

.4 Use of ICT resources

- **How often do you use the following resources indicated in section B?**

Resource	Daily	Weekly	Monthly	Quarterly
Network drive	.	.	.	.

IT System (SAP GRC)	.	.	.	.
Internet explorer	.	.	.	.
Email	.	.	.	.
Ms Teams	.	.	.	.

- **Please indicate the level of your skills relating to the resources in section B using the below likert scale:**

Limited	Basic	Proficient	Advanced	Expert
1	2	3	4	

IT Skill	Limited	Basic	Proficient	Advanced	Expert
Excel/ spreadsheet	.	.	.	.	.
Word	.	.	.	.	.
Powerpoint	.	.	.	.	.

Email	.	.	.	.	.
Internet explorer	.	.	.	.	.
Ms Teams	.	.	.	.	.

- **What do you use the following resources for (indicate for what purpose the IT resource is used for)?**

IT Resource	Use of the resource
Excel/ spreadsheet	
Word	
Powerpoint	
Email	
Internet explorer	
Ms Teams	

- **Why are you not using the ICT resources provided (please indicate the reason next to the resource)?**

IT Resource	Reasons for not using the resource

Excel/ spreadsheet	
Word	
PowerPoint	
Email	
Internet search	
Ms Teams	

- **Do you believe that having access to ICT resources is important?**

Strongly agree	Agree	Don’t know	Disagree	Strongly disagree

- **Do you believe that using ICT resources in risk management useful?**

Strongly agree	Agree	Don’t know	Disagree	Strongly disagree

Section 3: Perceived impact of ICT on implementing risk management

3.1 Please rate the following statements regarding the use of technology in implementing risk management activities.

Strongly agree	Agree	Don't know	Disagree	Strongly disagree

Impact:	Strongly agree	Agree	Don't know	Disagree	Strongly disagree
Identify and assess risks accurately	.	.	.	.	.
To manage and monitor identified risks better	.	.	.	.	.
Communicate risk activities efficiently	.	.	.	.	.
Assign responsibility and accountability to relevant managers accurately	.	.	.	.	.
Ability to define risk appetite levels	.	.	.	.	.

Improve reporting of risks	.	.	.	.	.
Allows easy submission of the portfolio of evidence	.	.	.	.	.
Allows to propose emerging risks in a timely manner	.	.	.	.	.
Effective capturing of quarterly progress against mitigations	.	.	.	.	.

Section 4: Challenges experienced by the users in using ICT

4..1 In your own view, what are the challenges affecting the use of ICT in risk management within the department?

____

____

____

4.2 How do you think these challenges can be addressed?

____

____

____

____

____

4.3 In your own view, what would be the benefits of addressing these challenges?

____

____

____

Thank you for completing the questionnaire.

Appendix G Interview questions

BACKGROUND

I am conducting research on above subject towards fulfilling the MTech in Information Technology in UNISA. The intention of this interview is to understand and determine whether integrating technology during the implementation of day-to-day risk management activities, has an impact on risk management effectiveness. To collect accurate and relevant data, I would like to ask the following questions.

Please be reminded that the questions asked during this interview will be treated as confidential.

Thank you for participating in this interview.

QUESTIONS:

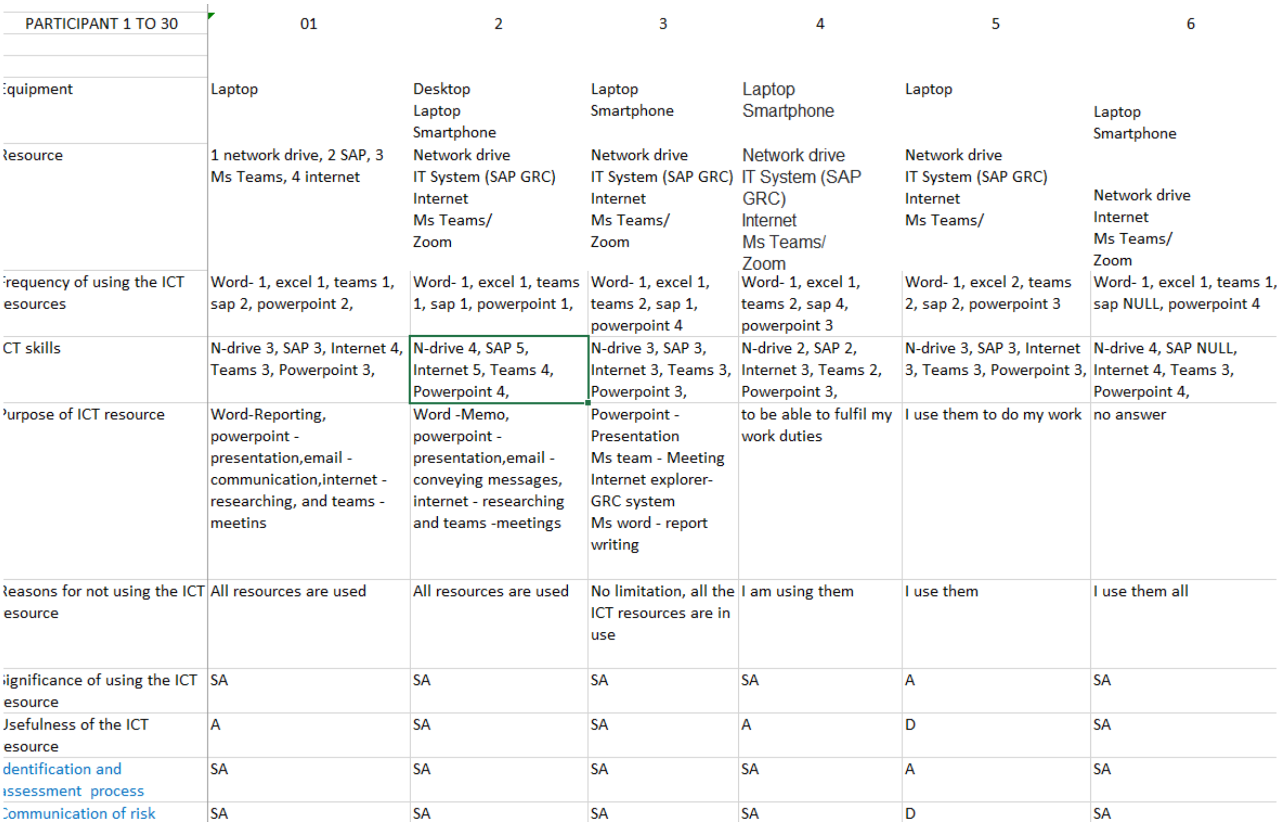
	NOTES
• Tell me about your role in risk management.	
• Do you have access to any ICT tools e.g. computer, system, internet etc?	
• How do you use ICT tools in your daily risk management activities?	
• Is ICT playing an effective role in implementing risk management activities?	
• What challenges do you have in using ICT tools in risk management?	
• What is the future of using ICT tools in risk management?	

	• Do you have any additional information you would like to share?	
Thank you for participating in this interview, your input is appreciated.		

Appendix H: Interview Schedule

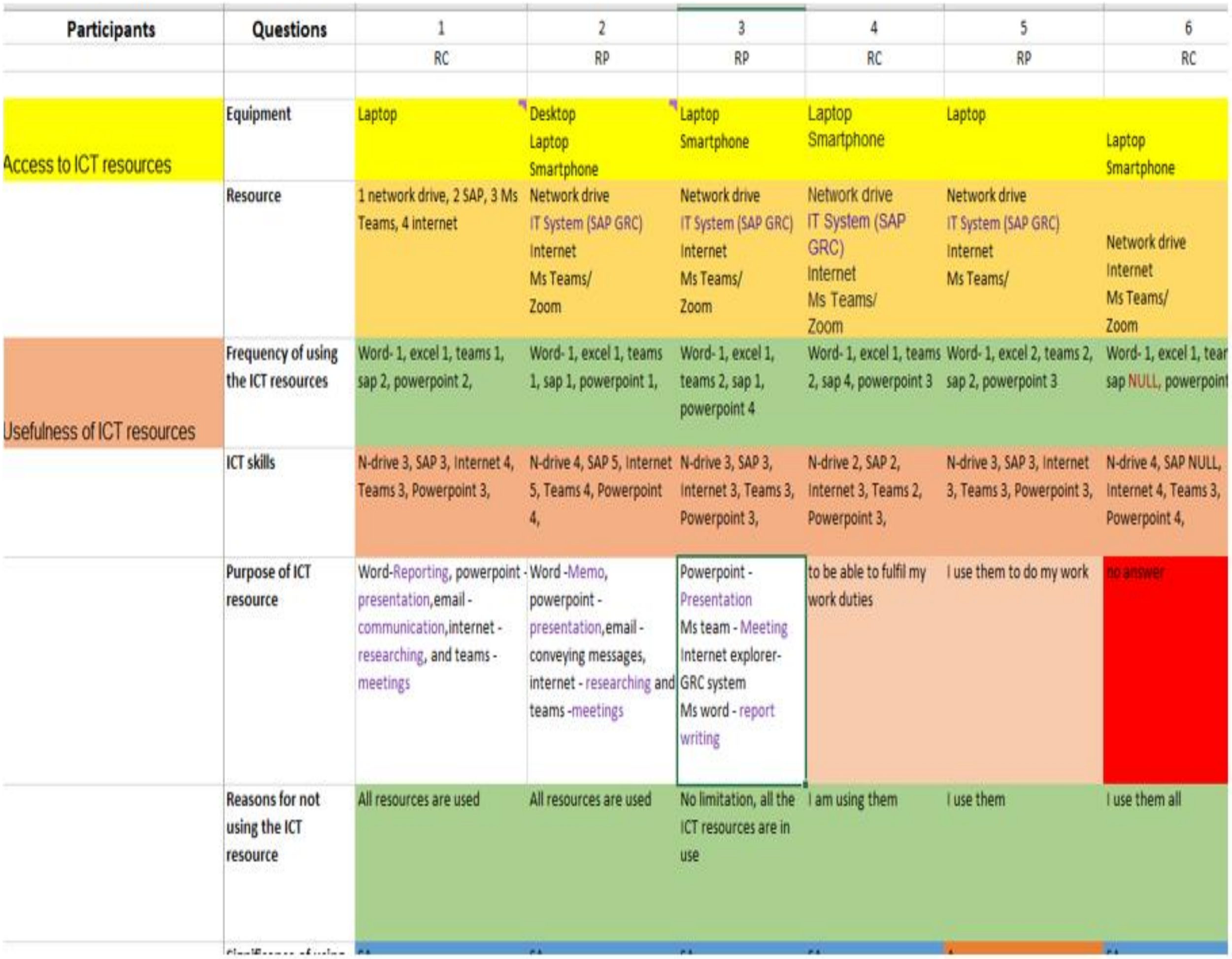
Participants	ROLE	Date of the interview	Time
A	Risk Practitioner	12 November 2020	13h00
B	Risk Practitioner	13 November 2020	12h00
C	Risk Practitioner	13 November 2020	14h00
D	Risk Champion	18 November 2020	12h30
E	Risk Practitioner	17 November 2020	09h00
F	Risk Practitioner	17 November 2020	11h00
G	Risk Champion	19 November 2020	11h00
H	Risk Champion	19 November 2020	10h00
I	Risk Champion	20 November 2020	15h00
J	Risk Champion	23 November 2020	09h00

Appendix I: Raw data from the survey (the spreadsheet captured all the thirty participants – this is an extract)



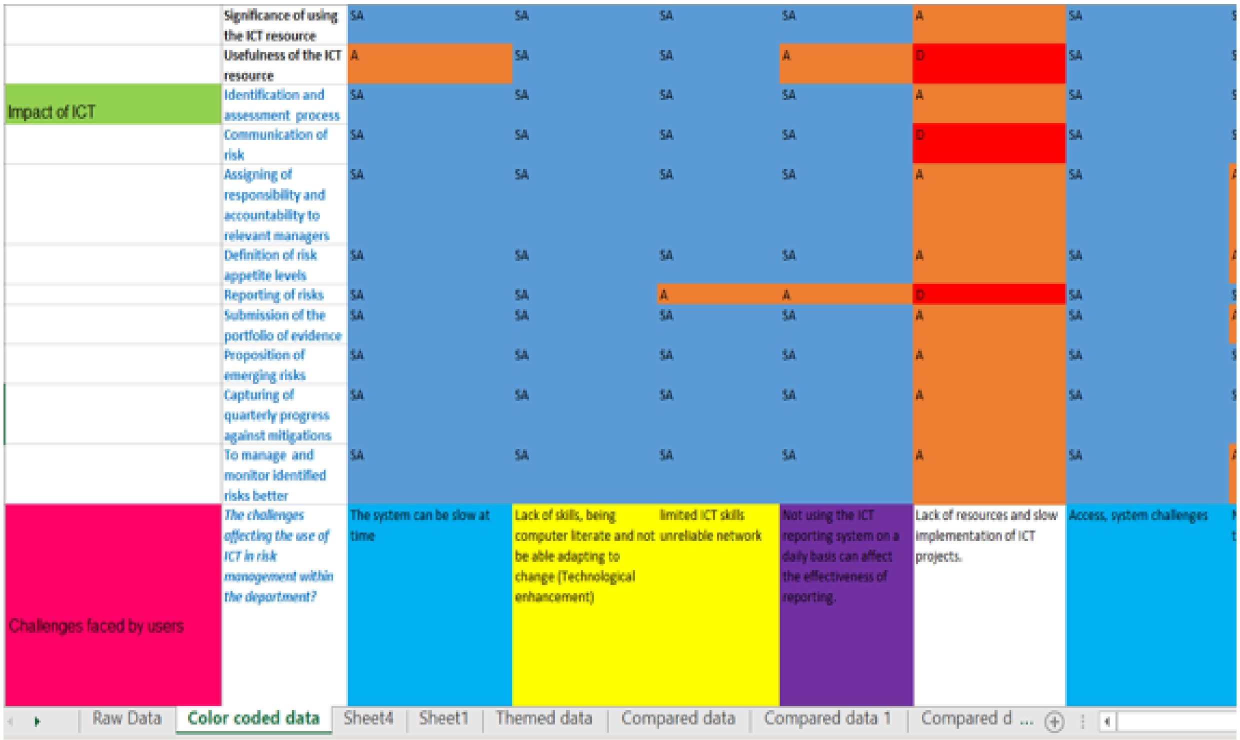
PARTICIPANT 1 TO 30	01	2	3	4	5	6
Equipment	Laptop	Desktop Laptop Smartphone	Laptop Smartphone	Laptop Smartphone	Laptop	Laptop Smartphone
Resource	1 network drive, 2 SAP, 3 Ms Teams, 4 internet	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/	Network drive Internet Ms Teams/ Zoom
Frequency of using the ICT esources	Word- 1, excel 1, teams 1, sap 2, powerpoint 2,	Word- 1, excel 1, teams 1, sap 1, powerpoint 1,	Word- 1, excel 1, teams 2, sap 1, powerpoint 4	Word- 1, excel 1, teams 2, sap 4, powerpoint 3	Word- 1, excel 2, teams 2, sap 2, powerpoint 3	Word- 1, excel 1, teams 1, sap NULL, powerpoint 4
ICT skills	N-drive 3, SAP 3, Internet 4, Teams 3, Powerpoint 3,	N-drive 4, SAP 5, Internet 5, Teams 4, Powerpoint 4,	N-drive 3, SAP 3, Internet 3, Teams 3, Powerpoint 3,	N-drive 2, SAP 2, Internet 3, Teams 2, Powerpoint 3,	N-drive 3, SAP 3, Internet 3, Teams 3, Powerpoint 3,	N-drive 4, SAP NULL, Internet 4, Teams 3, Powerpoint 4,
Purpose of ICT resource	Word-Reporting, powerpoint - presentation,email - communication,internet - researching, and teams - meetins	Word -Memo, powerpoint - presentation,email - conveying messages, internet - researching and teams -meetings	Powerpoint - Presentation Ms team - Meeting Internet explorer- GRC system Ms word - report writing	to be able to fulfil my work duties	I use them to do my work	no answer
Reasons for not using the ICT esource	All resources are used	All resources are used	No limitation, all the ICT resources are in use	I am using them	I use them	I use them all
Significance of using the ICT esource	SA	SA	SA	SA	A	SA
Usefulness of the ICT esource	A	SA	SA	A	D	SA
Identification and assessment process	SA	SA	SA	SA	A	SA
Communication of risk	SA	SA	SA	SA	D	SA

Appendix J.1: Initial coded data from the survey

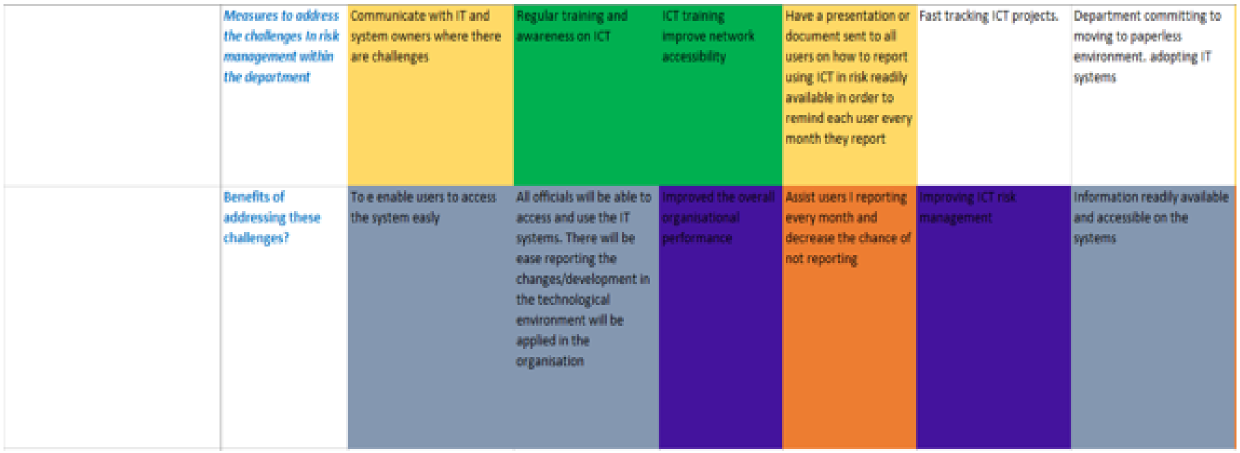


Participants	Questions	1	2	3	4	5	6
		RC	RP	RP	RC	RP	RC
Access to ICT resources	Equipment	Laptop	Desktop Laptop Smartphone	Laptop Smartphone	Laptop Smartphone	Laptop	Laptop Smartphone
	Resource	1 network drive, 2 SAP, 3 Ms Teams, 4 internet	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/ Zoom	Network drive IT System (SAP GRC) Internet Ms Teams/	Network drive Internet Ms Teams/ Zoom
Usefulness of ICT resources	Frequency of using the ICT resources	Word- 1, excel 1, teams 1, sap 2, powerpoint 2,	Word- 1, excel 1, teams 1, sap 1, powerpoint 1,	Word- 1, excel 1, teams 2, sap 1, powerpoint 4	Word- 1, excel 1, teams 2, sap 4, powerpoint 3	Word- 1, excel 2, teams 2, sap 2, powerpoint 3	Word- 1, excel 1, tear sap NULL, powerpoint
	ICT skills	N-drive 3, SAP 3, Internet 4, Teams 3, Powerpoint 3,	N-drive 4, SAP 5, Internet 5, Teams 4, Powerpoint 4,	N-drive 3, SAP 3, Internet 3, Teams 3, Powerpoint 3,	N-drive 2, SAP 2, Internet 3, Teams 2, Powerpoint 3,	N-drive 3, SAP 3, Internet 3, Teams 3, Powerpoint 3,	N-drive 4, SAP NULL, Internet 4, Teams 3, Powerpoint 4,
	Purpose of ICT resource	Word-Reporting, powerpoint - presentation,email - communication,internet - researching, and teams - meetings	Word -Memo, powerpoint - presentation,email - conveying messages, internet - researching and teams -meetings	Powerpoint - Presentation Ms team - Meeting Internet explorer- GRC system Ms word - report writing	to be able to fulfil my work duties	I use them to do my work	no answer
	Reasons for not using the ICT resource	All resources are used	All resources are used	No limitation, all the ICT resources are in use	I am using them	I use them	I use them all
	Significance of using	SA	SA	SA	SA	A	SA

Appendix J.2: Initial coded data from the survey

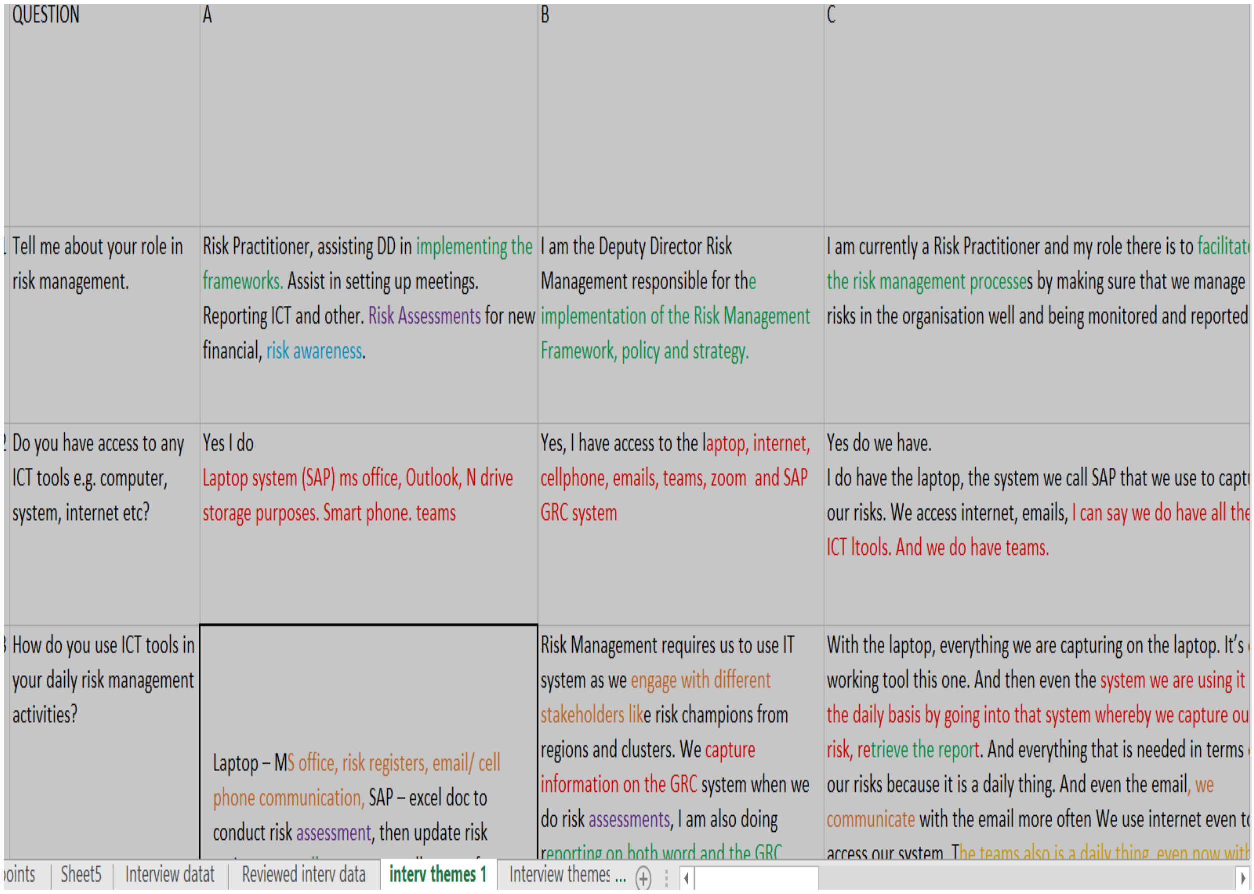


	Significance of using the ICT resource	SA	SA	SA	SA	A	SA
	Usefulness of the ICT resource	A	SA	SA	A	D	SA
Impact of ICT	Identification and assessment process	SA	SA	SA	SA	A	SA
	Communication of risk	SA	SA	SA	SA	D	SA
	Assigning of responsibility and accountability to relevant managers	SA	SA	SA	SA	A	SA
	Definition of risk appetite levels	SA	SA	SA	SA	A	SA
	Reporting of risks	SA	SA	A	A	D	SA
	Submission of the portfolio of evidence	SA	SA	SA	SA	A	SA
	Proposition of emerging risks	SA	SA	SA	SA	A	SA
	Capturing of quarterly progress against mitigations	SA	SA	SA	SA	A	SA
	To manage and monitor identified risks better	SA	SA	SA	SA	A	SA
Challenges faced by users	*The challenges affecting the use of ICT in risk management within the department?*	The system can be slow at time	Lack of skills, being computer literate and not be able adapting to change (Technological enhancement)	limited ICT skills unreliable network	Not using the ICT reporting system on a daily basis can affect the effectiveness of reporting.	Lack of resources and slow implementation of ICT projects.	Access, system challenges



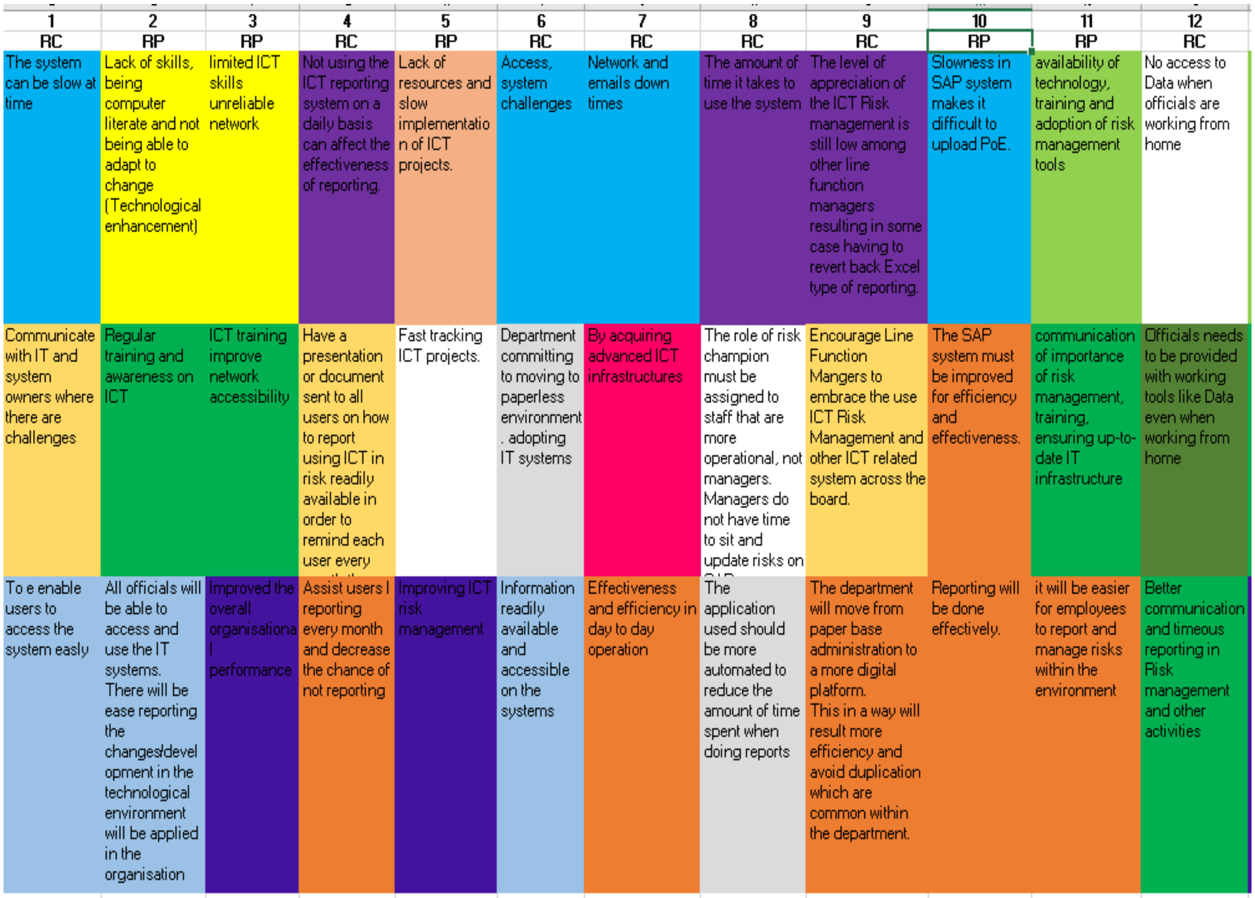
	Measures to address the challenges In risk management within the department	Communicate with IT and system owners where there are challenges	Regular training and awareness on ICT	ICT training improve network accessibility	Have a presentation or document sent to all users on how to report using ICT in risk readily available in order to remind each user every month they report	Fast tracking ICT projects.	Department committing to moving to paperless environment. adopting IT systems
	Benefits of addressing these challenges?	To e enable users to access the system easly	All officials will be able to access and use the IT systems. There will be ease reporting the changes/development in the technological environment will be applied in the organisation	Improved the overall organisational performance	Assist users I reporting every month and decrease the chance of not reporting	Improving ICT risk management	Information readily available and accessible on the systems

Appendix J.3: Initial coded data from the interviews



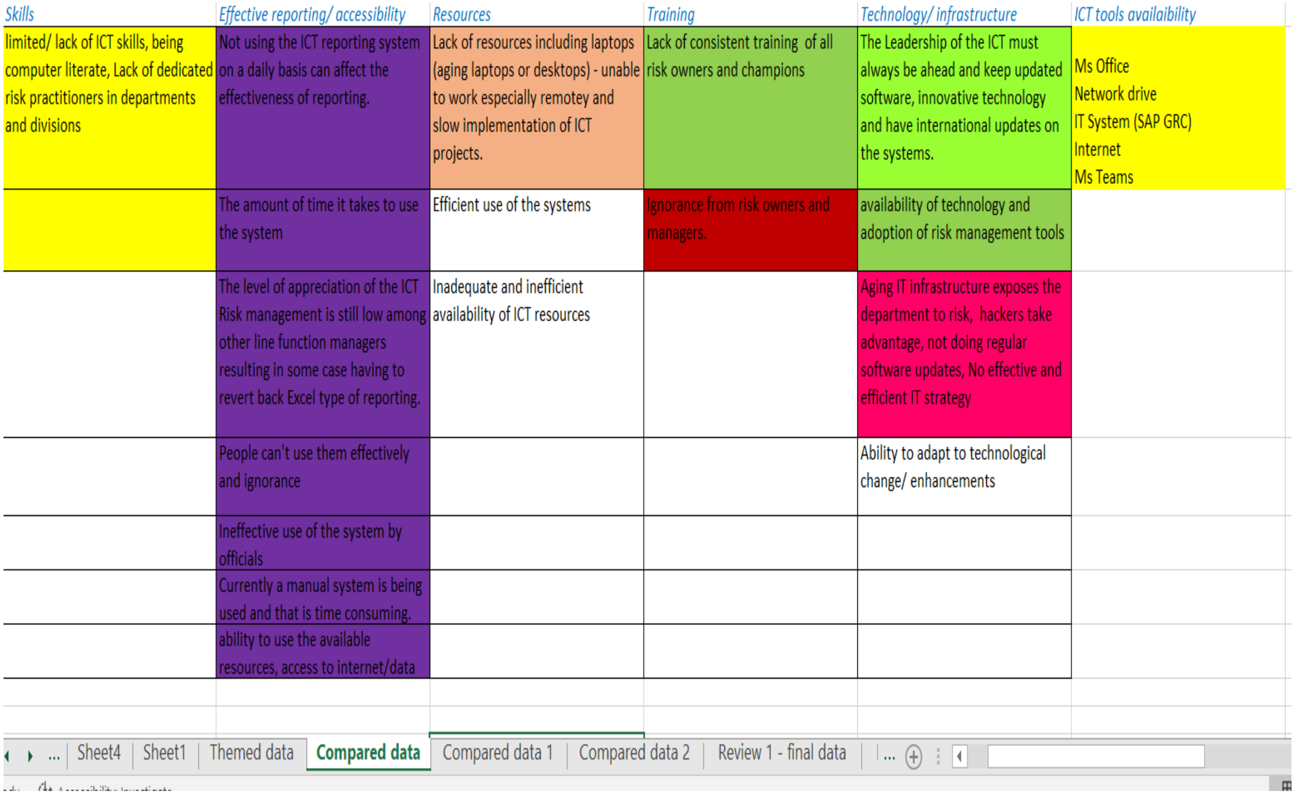
QUESTION	A	B	C
1 Tell me about your role in risk management.	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy and strategy.	I am currently a Risk Practitioner and my role there is to facilitate the risk management processes by making sure that we manage risks in the organisation well and being monitored and reported
2 Do you have access to any ICT tools e.g. computer, system, internet etc?	Yes I do Laptop system (SAP) ms office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cellphone, emails, teams, zoom and SAP GRC system	Yes do we have. I do have the laptop, the system we call SAP that we use to captu our risks. We access internet, emails, I can say we do have all the ICT ltools. And we do have teams.
3 How do you use ICT tools in your daily risk management activities?	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC	With the laptop, everything we are capturing on the laptop. It's working tool this one. And then even the system we are using it the daily basis by going into that system whereby we capture ou risk, retrieve the report. And everything that is needed in terms our risks because it is a daily thing. And even the email, we communicate with the email more often We use internet even to access our system. The teams also is a daily thing, even now with

Appendix K: First level themes - survey



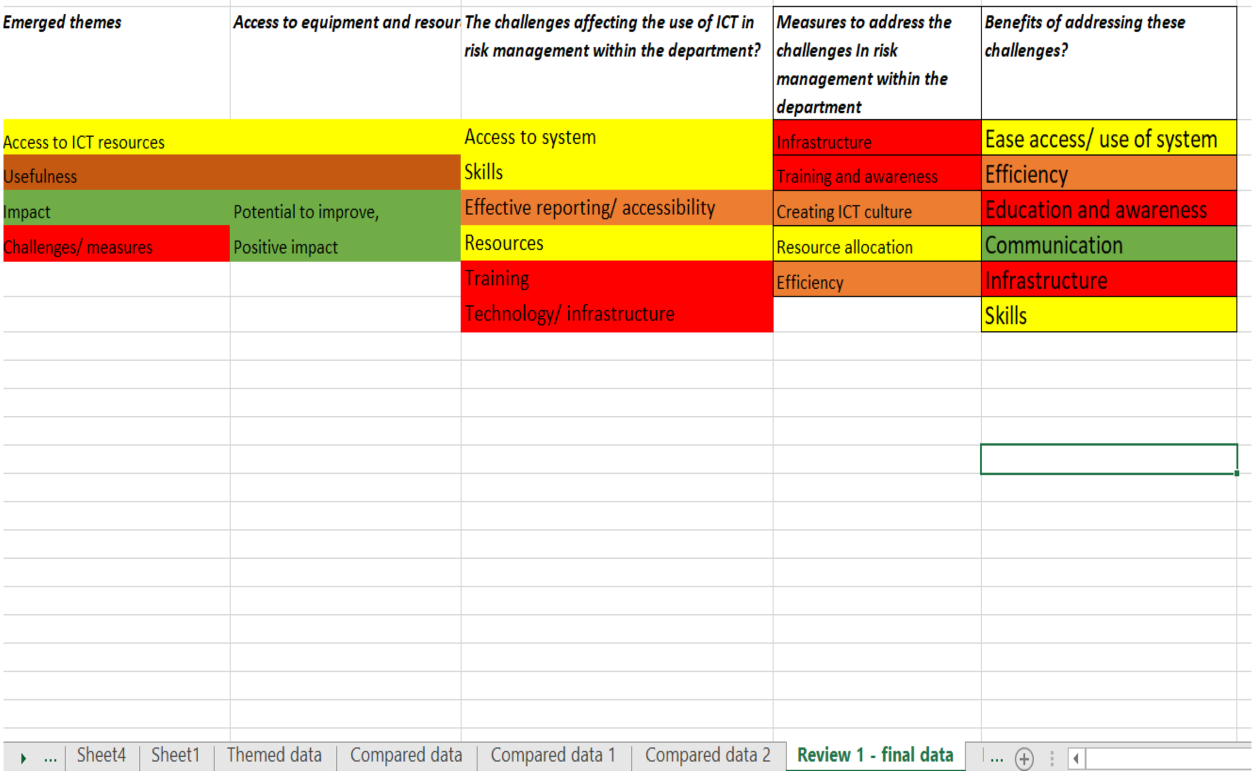
1	2	3	4	5	6	7	8	9	10	11	12
RC	RP	RP	RC	RP	RC	RC	RC	RC	RP	RP	RC
The system can be slow at time	Lack of skills, being computer literate and not being able to adapt to change (Technological enhancement)	limited ICT skills unreliable network	Not using the ICT reporting system on a daily basis can affect the effectiveness of reporting.	Lack of resources and slow implementation of ICT projects.	Access, system challenges	Network and emails down times	The amount of time it takes to use the system	The level of appreciation of the ICT Risk management is still low among other line function managers resulting in some case having to revert back Excel type of reporting.	Slowness in SAP system makes it difficult to upload PoE.	availability of technology, training and adoption of risk management tools	No access to Data when officials are working from home
Communicate with IT and system owners where there are challenges	Regular training and awareness on ICT	ICT training improve network accessibility	Have a presentation or document sent to all users on how to report using ICT in risk readily available in order to remind each user every	Fast tracking ICT projects.	Department committing to moving to paperless environment . adopting IT systems	By acquiring advanced ICT infrastructures	The role of risk champion must be assigned to staff that are more operational, not managers. Managers do not have time to sit and update risks on	Encourage Line Function Mangers to embrace the use ICT Risk Management and other ICT related system across the board.	The SAP system must be improved for efficiency and effectiveness.	communication of importance of risk management, training, ensuring up-to-date IT infrastructure	Officials needs to be provided with working tools like Data even when working from home
To e enable users to access the system easly	All officials will be able to access and use the IT systems. There will be ease reporting the changes/development in the technological environment will be applied in the organisation	Improved the overall organisational performance	Assist users l reporting every month and decrease the chance of not reporting	Improving ICT risk management	Information readily available and accessible on the systems	Effectiveness and efficiency in day to day operation	The application used should be more automated to reduce the amount of time spent when doing reports	The department will move from paper base administration to a more digital platform. This in a way will result more efficiency and avoid duplication which are common within the department.	Reporting will be done effectively.	it will be easier for employees to report and manage risks within the environment	Better communication and timeous reporting in Risk management and other activities

Appendix L: Reduced themes - survey



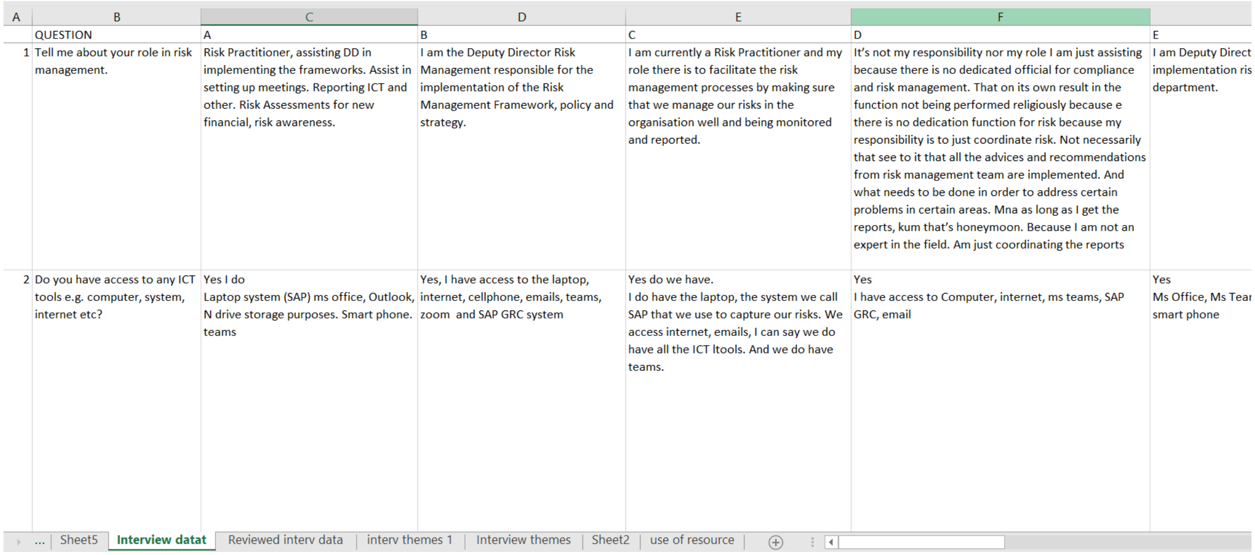
Skills	Effective reporting/ accessibility	Resources	Training	Technology/ infrastructure	ICT tools availaibility
limited/ lack of ICT skills, being computer literate, Lack of dedicated risk practitioners in departments and divisions	Not using the ICT reporting system on a daily basis can affect the effectiveness of reporting.	Lack of resources including laptops (aging laptops or desktops) - unable to work especially remotey and slow implementation of ICT projects.	Lack of consistent training of all risk owners and champions	The Leadership of the ICT must always be ahead and keep updated software, innovative technology and have international updates on the systems.	Ms Office Network drive IT System (SAP GRC) Internet Ms Teams
	The amount of time it takes to use the system	Efficient use of the systems	Ignorance from risk owners and managers.	availability of technology and adoption of risk management tools	
	The level of appreciation of the ICT Risk management is still low among other line function managers resulting in some case having to revert back Excel type of reporting.	Inadequate and inefficient availability of ICT resources		Aging IT infrastructure exposes the department to risk, hackers take advantage, not doing regular software updates, No effective and efficient IT strategy	
	People can't use them effectively and ignorance			Ability to adapt to technological change/ enhancements	
	Ineffective use of the system by officials				
	Currently a manual system is being used and that is time consuming.				
	ability to use the available resources, access to internet/data				

Appendix M: Emerged key themes - survey

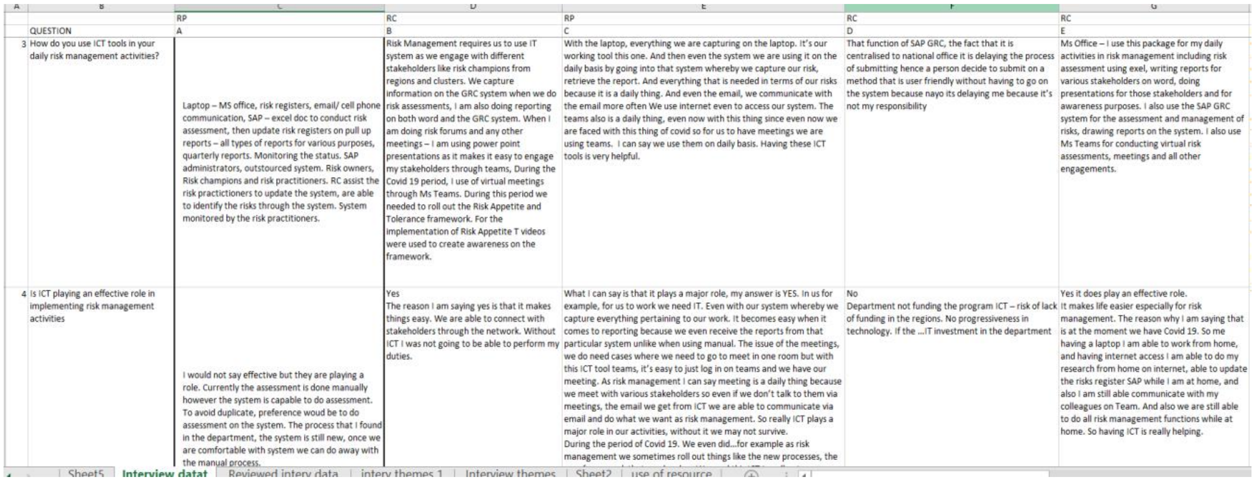


Emerged themes	*Access to equipment and resour*	*The challenges affecting the use of ICT in risk management within the department?*	*Measures to address the challenges In risk management within the department*	*Benefits of addressing these challenges?*
Access to ICT resources		Access to system	Infrastructure	Ease access/ use of system
Usefulness		Skills	Training and awareness	Efficiency
Impact	Potential to improve,	Effective reporting/ accessibility	Creating ICT culture	Education and awareness
Challenges/ measures	Positive impact	Resources	Resource allocation	Communication
		Training	Efficiency	Infrastructure
		Technology/ infrastructure		Skills

Appendix N: Raw data from the interviews

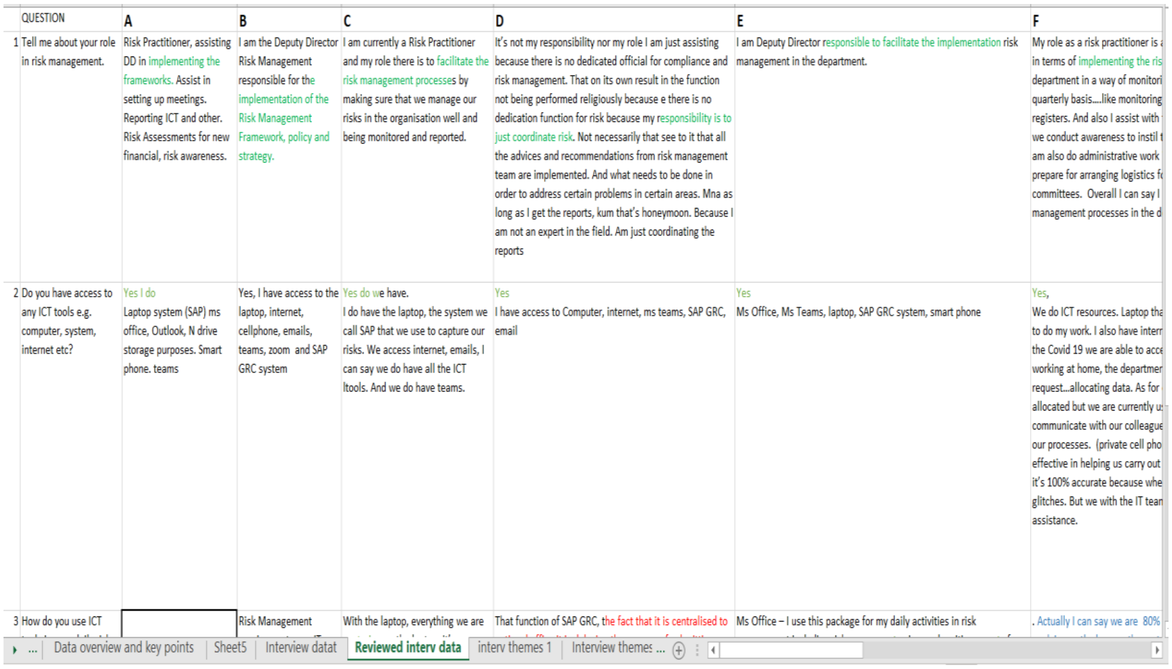


A	B	C	D	E	F	
	QUESTION	A	B	C	D	E
1	Tell me about your role in risk management.	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy and strategy.	I am currently a Risk Practitioner and my role there is to facilitate the risk management processes by making sure that we manage our risks in the organisation well and being monitored and reported.	It's not my responsibility nor my role I am just assisting because there is no dedicated official for compliance and risk management. That on its own result in the function not being performed religiously because e there is no dedication function for risk because my responsibility is to just coordinate risk. Not necessarily that see to it that all the advices and recommendations from risk management team are implemented. And what needs to be done in order to address certain problems in certain areas. Mna as long as I get the reports, kum that's honeymoon. Because I am not an expert in the field. Am just coordinating the reports	I am Deputy Direct implementation ris department.
2	Do you have access to any ICT tools e.g. computer, system, internet etc?	Yes I do Laptop system (SAP) ms office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cellphone, emails, teams, zoom and SAP GRC system	Yes do we have. I do have the laptop, the system we call SAP that we use to capture our risks. We access internet, emails, I can say we do have all the ICT ltools. And we do have teams.	Yes I have access to Computer, internet, ms teams, SAP GRC, email	Yes Ms Office, Ms Tear smart phone

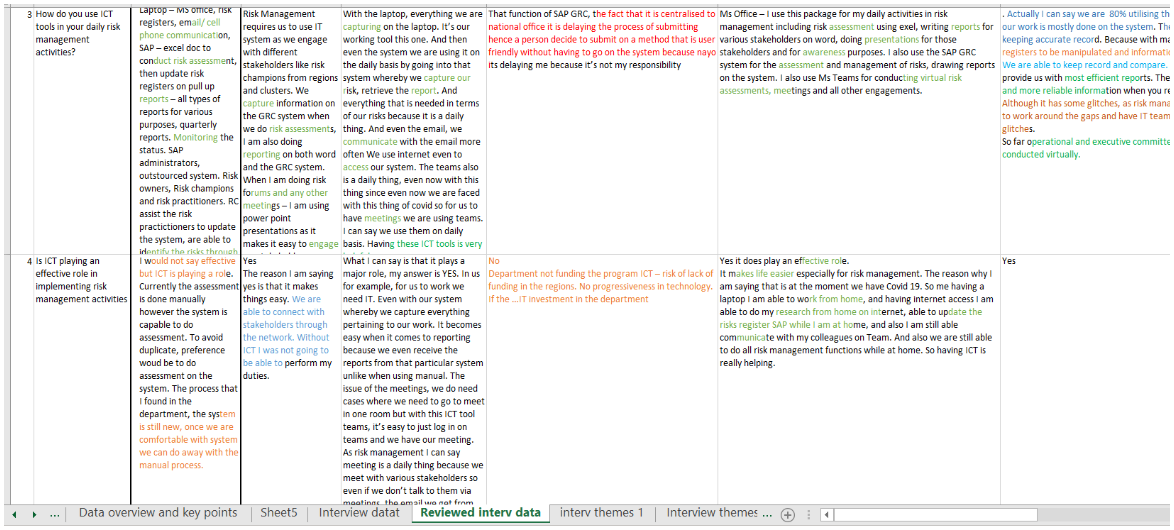


A	B	C	D	E	F	G
		RP	RC	RP	RC	RC
	QUESTION	A	B	C	D	E
3	How do you use ICT tools in your daily risk management activities?	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk registers on pull up reports – all types of reports for various purposes, quarterly reports. Monitoring the status. SAP administrators, outstourced system. Risk owners, Risk champions and risk practitioners. RC assist the risk practictioners to update the system, are able to identify the risks through the system. System monitored by the risk practitioners.	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC system. When I am doing risk forums and any other meetings – I am using power point presentations as it makes it easy to engage my stakeholders through teams, During the Covid 19 period, I use of virtual meetings through Ms Teams. During this period we needed to roll out the Risk Appetite and Tolerance framework. For the implementation of Risk Appetite T videos were used to create awareness on the framework.	With the laptop, everything we are capturing on the laptop. It's our working tool this one. And then even the system we are using it on the daily basis by going into that system whereby we capture our risk, retrieve the report. And everything that is needed in terms of our risks because it is a daily thing. And even the email, we communicate with the email more often We use internet even to access our system. The teams also is a daily thing, even now with this thing since even now we are faced with this thing of covid so for us to have meetings we are using teams. I can say we use them on daily basis. Having these ICT tools is very helpful.	That function of SAP GRC, the fact that it is centralised to national office it is delaying the process of submitting hence a person decide to submit on a method that is user friendly without having to go on the system because nayo its delaying me because it's not my responsibility	Ms Office – I use this package for my daily activities in risk management including risk assessment using exel, writing reports for various stakeholders on word, doing presentations for those stakeholders and for awareness purposes. I also use the SAP GRC system for the assessment and management of risks, drawing reports on the system. I also use Ms Teams for conducting virtual risk assessments, meetings and all other engagements.
4	Is ICT playing an effective role in implementing risk management activities	I would not say effective but they are playing a role. Currently the assessment is done manually however the system is capable to do assessment. To avoid duplicate, preference woud be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	Yes The reason I am saying yes is that it makes things easy. We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	What I can say is that it plays a major role, my answer is YES. In us for example, for us to work we need IT. Even with our system whereby we capture everything pertaining to our work. It becomes easy when it comes to reporting because we even receive the reports from that particular system unlike when using manual. The issue of the meetings, we do need cases where we need to go to meet in one room but with this ICT tool teams, it's easy to just log in on teams and we have our meeting. As risk management I can say meeting is a daily thing because we meet with various stakeholders so even if we don't talk to them via meetings, the email we get from ICT we are able to communicate via email and do what we want as risk management. So really ICT plays a major role in our activities, without it we may not survive. During the period of Covid 19. We even did...for example as risk management we sometimes roll out things like the new processes, the	No Department not funding the program ICT – risk of lack of funding in the regions. No progressiveness in technology. If the ...IT investment in the department	Yes it does play an effective role. It makes life easier especially for risk management. The reason why I am saying that is at the moment we have Covid 19. So me having a laptop I am able to work from home, and having internet access I am able to do my research from home on internet, able to update the risks register SAP while I am at home, and also I am still able communicate with my colleagues on Team. And also we are still able to do all risk management functions while at home. So having ICT is really helping.

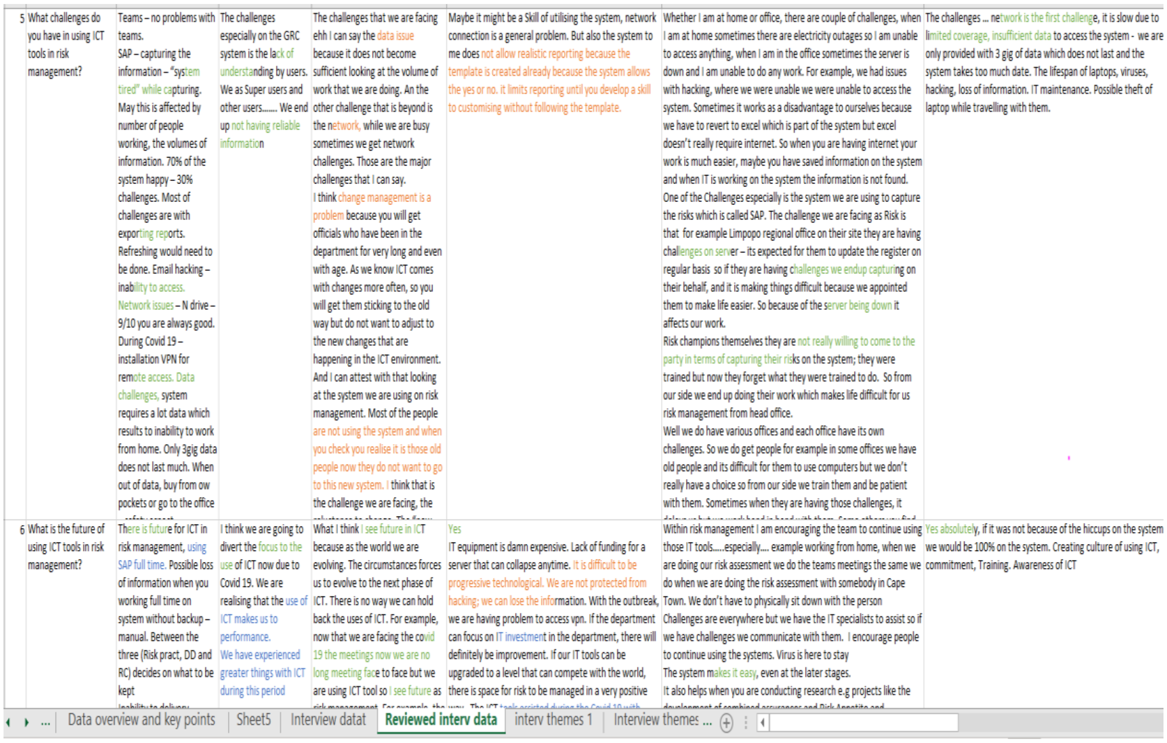
Appendix O: First level themes - interviews



	QUESTION	A	B	C	D	E	F
1	Tell me about your role in risk management.	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy and strategy.	I am currently a Risk Practitioner and my role there is to facilitate the risk management processes by making sure that we manage our risks in the organisation well and being monitored and reported.	It's not my responsibility nor my role I am just assisting because there is no dedicated official for compliance and risk management. That on its own result in the function not being performed religiously because e there is no dedication function for risk because my responsibility is to just coordinate risk. Not necessarily that see to it that all the advices and recommendations from risk management team are implemented. And what needs to be done in order to address certain problems in certain areas. Mna as long as I get the reports, kum that's honeymoon. Because I am not an expert in the field. Am just coordinating the reports	I am Deputy Director responsible to facilitate the implementation risk management in the department.	My role as a risk practitioner is a in terms of implementing the ris department in a way of monitori quarterly basis....like monitoring registers. And also I assist with we conduct awareness to instil t am also do administrative work prepare for arranging logistics fo committees. Overall I can say I management processes in the d
2	Do you have access to any ICT tools e.g. computer, system, internet etc?	Yes I do Laptop system (SAP) ms office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cellphone, emails, teams, zoom and SAP GRC system	Yes do we have. I do have the laptop, the system we call SAP that we use to capture our risks. We access internet, emails, I can say we do have all the ICT Itools. And we do have teams.	Yes I have access to Computer, internet, ms teams, SAP GRC, email	Yes Ms Office, Ms Teams, laptop, SAP GRC system, smart phone	Yes, We do ICT resources. Laptop tha to do my work. I also have intern the Covid 19 we are able to acce working at home, the departmen request...allocating data. As for allocated but we are currently u communicate with our colleague our processes. (private cell pho effective in helping us carry out it's 100% accurate because whe glitches. But we with the IT tean assistance.
3	How do you use ICT		Risk Management	With the laptop, everything we are	That function of SAP GRC, the fact that it is centralised to	Ms Office – I use this package for my daily activities in risk	. Actually I can say we are 80%

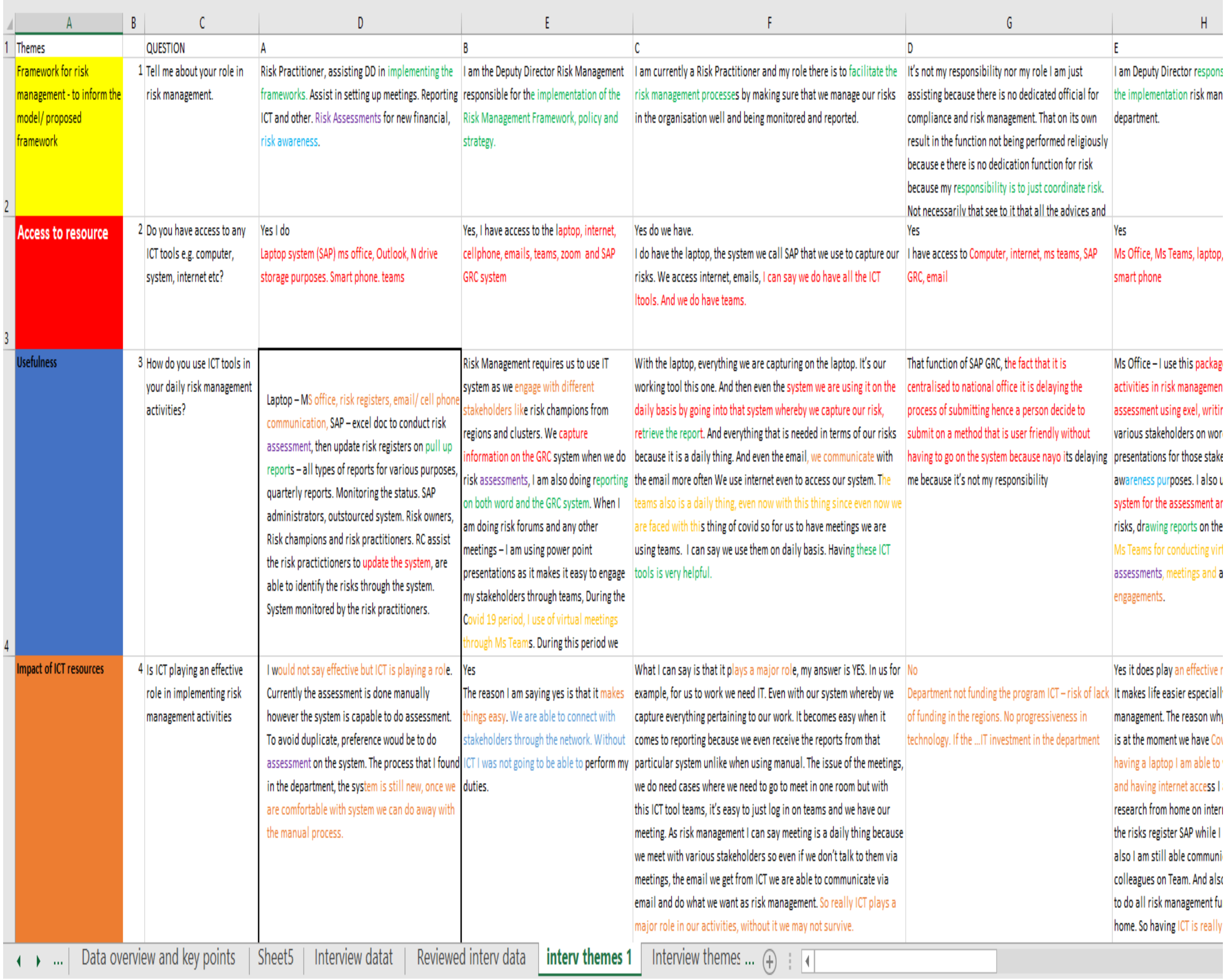


3	How do you use ICT tools in your daily risk management activities?	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk registers on pull up reports – all types of reports for various purposes, quarterly reports. Monitoring the status. SAP administrators, outstourced system. Risk owners, Risk champions and risk practitioners. RC assist the risk practictioners to update the system, are able to identify the risks through	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC system. When I am doing risk forums and any other meetings – I am using power point presentations as it makes it easy to engage	With the laptop, everything we are capturing on the laptop. It's our working tool this one. And then even the system we are using it on the daily basis by going into that system whereby we capture our risk, retrieve the report. And everything that is needed in terms of our risks because it is a daily thing. And even the email, we communicate with the email more often We use internet even to access our system. The teams also is a daily thing, even now with this thing since even now we are faced with this thing of covid so for us to have meetings we are using teams. I can say we use them on daily basis. Having these ICT tools is very	That function of SAP GRC, the fact that it is centralised to national office it is delaying the process of submitting hence a person decide to submit on a method that is user friendly without having to go on the system because nayo its delaying me because it's not my responsibility	Ms Office – I use this package for my daily activities in risk management including risk assessment using exel, writing reports for various stakeholders on word, doing presentations for those stakeholders and for awareness purposes. I also use the SAP GRC system for the assessment and management of risks, drawing reports on the system. I also use Ms Teams for conducting virtual risk assessments, meetings and all other engagements.	. Actually I can say we are 80% utilising th our work is mostly done on the system. The keeping accurate record. Because with ma registers to be manipulated and informatio We are able to keep record and compare. provide us with most efficient reports. The and more reliable information when you re Although it has some glitches, as risk mana to work around the gaps and have IT team glitches. So far operational and executive committe conducted virtually.
4	Is ICT playing an effective role in implementing risk management activities	I would not say effective but ICT is playing a role. Currently the assessment is done manually however the system is capable to do assessment. To avoid duplicate, preference woud be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	Yes The reason I am saying yes is that it makes things easy. We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	What I can say is that it plays a major role, my answer is YES. In us for example, for us to work we need IT. Even with our system whereby we capture everything pertaining to our work. It becomes easy when it comes to reporting because we even receive the reports from that particular system unlike when using manual. The issue of the meetings, we do need cases where we need to go to meet in one room but with this ICT tool teams, it's easy to just log in on teams and we have our meeting. As risk management I can say meeting is a daily thing because we meet with various stakeholders so even if we don't talk to them via meetings, the email we get from	No Department not funding the program ICT – risk of lack of funding in the regions. No progressiveness in technology. If the ...IT investment in the department	Yes it does play an effective role. It makes life easier especially for risk management. The reason why I am saying that is at the moment we have Covid 19. So me having a laptop I am able to work from home, and having internet access I am able to do my research from home on internet, able to update the risks register SAP while I am at home, and also I am still able communicate with my colleagues on Team. And also we are still able to do all risk management functions while at home. So having ICT is really helping.	Yes



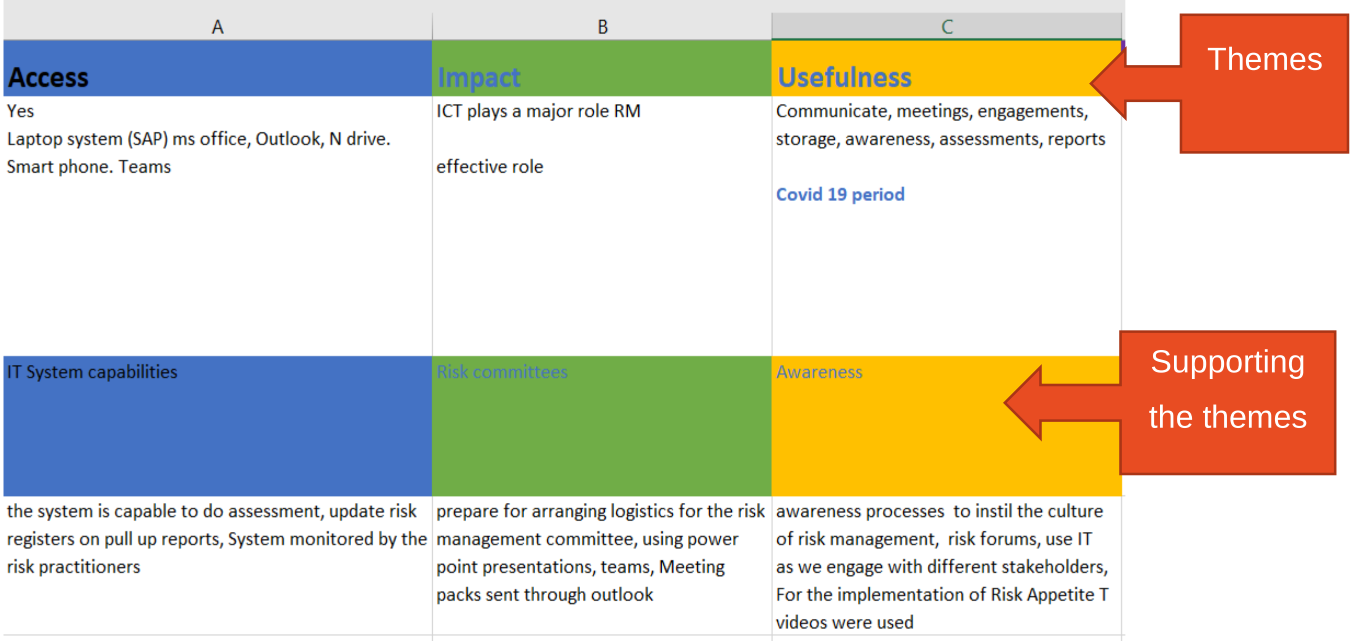
5	What challenges do you have in using ICT tools in risk management?	Teams – no problems with teams. SAP – capturing the information – "system tired" while capturing. May this is affected by number of people working, the volumes of information. 70% of the system happy – 30% challenges. Most of challenges are with exporting reports. Refreshing would need to be done. Email hacking – inability to access. Network issues – N drive – 9/10 you are always good. During Covid 19 – installation VPN for remote access. Data challenges, system requires a lot data which results to inability to work from home. Only 3gig data does not last much. When out of data, buy from ow pockets or go to the office	The challenges especially on the GRC system is the lack of understanding by users. We as Super users and other users……. We end up not having reliable information	The challenges that we are facing ehh I can say the data issue because it does not become sufficient looking at the volume of work that we are doing. An the other challenge that is beyond is the network, while we are busy sometimes we get network challenges. Those are the major challenges that I can say. I think change management is a problem because you will get officials who have been in the department for very long and even with age. As we know ICT comes with changes more often, so you will get them sticking to the old way but do not want to adjust to the new changes that are happening in the ICT environment. And I can attest with that looking at the system we are using on risk management. Most of the people are not using the system and when you check you realise it is those old people now they do not want to go to this new system. I think that is the challenge we are facing, the	Maybe it might be a Skill of utilising the system, network connection is a general problem. But also the system to me does not allow realistic reporting because the template is created already because the system allows the yes or no. it limits reporting until you develop a skill to customising without following the template.	Whether I am at home or office, there are couple of challenges, when I am at home sometimes there are electricity outages so I am unable to access anything, when I am in the office sometimes the server is down and I am unable to do any work. For example, we had issues with hacking, where we were unable we were unable to access the system. Sometimes it works as a disadvantage to ourselves because we have to revert to excel which is part of the system but excel doesn't really require internet. So when you are having internet your work is much easier, maybe you have saved information on the system and when IT is working on the system the information is not found. One of the Challenges especially is the system we are using to capture the risks which is called SAP. The challenge we are facing as Risk is that for example Limpopo regional office on their site they are having challenges on server – its expected for them to update the register on regular basis so if they are having challenges we endup capturing on their behalf, and it is making things difficult because we appointed them to make life easier. So because of the server being down it affects our work. Risk champions themselves they are not really willing to come to the party in terms of capturing their risks on the system; they were trained but now they forget what they were trained to do. So from our side we end up doing their work which makes life difficult for us risk management from head office. Well we do have various offices and each office have its own challenges. So we do get people for example in some offices we have old people and its difficult for them to use computers but we don't really have a choice so from our side we train them and be patient with them. Sometimes when they are having those challenges, it	The challenges … network is the first challenge, it is slow due to limited coverage, insufficient data to access the system - we are only provided with 3 gig of data which does not last and the system takes too much date. The lifespan of laptops, viruses, hacking, loss of information. IT maintenance. Possible theft of laptop while travelling with them.
6	What is the future of using ICT tools in risk management?	There is future for ICT in risk management, using SAP full time. Possible loss of information when you working full time on system without backup – manual. Between the three (Risk pract, DD and RC) decides on what to be kept	I think we are going to divert the focus to the use of ICT now due to Covid 19. We are realising that the use of ICT makes us to performance. We have experienced greater things with ICT during this period	What I think I see future in ICT because as the world we are evolving. The circumstances forces us to evolve to the next phase of ICT. There is no way we can hold back the uses of ICT. For example, now that we are facing the covid 19 the meetings now we are no long meeting face to face but we are using ICT tool so I see future as	Yes IT equipment is damn expensive. Lack of funding for a server that can collapse anytime. It is difficult to be progressive technological. We are not protected from hacking; we can lose the information. With the outbreak, we are having problem to access vpn. If the department can focus on IT investment in the department, there will definitely be improvement. If our IT tools can be upgraded to a level that can compete with the world, there is space for risk to be managed in a very positive	Within risk management I am encouraging the team to continue using those IT tools…..especially…. example working from home, when we are doing our risk assessment we do the teams meetings the same we do when we are doing the risk assessment with somebody in Cape Town. We don't have to physically sit down with the person Challenges are everywhere but we have the IT specialists to assist so if we have challenges we communicate with them. I encourage people to continue using the systems. Virus is here to stay The system makes it easy, even at the later stages. It also helps when you are conducting research e.g projects like the	Yes absolutely, if it was not because of the hiccups on the system we would be 100% on the system. Creating culture of using ICT, commitment, Training. Awareness of ICT

Appendix P: Reduced themes - interviews



	A	B	C	D	E	F	G	H
1	Themes		QUESTION	A	B	C	D	E
2	Framework for risk management - to inform the model/ proposed framework	1	Tell me about your role in risk management.	Risk Practitioner, assisting DD in implementing the frameworks. Assist in setting up meetings. Reporting ICT and other. Risk Assessments for new financial, risk awareness.	I am the Deputy Director Risk Management responsible for the implementation of the Risk Management Framework, policy and strategy.	I am currently a Risk Practitioner and my role there is to facilitate the risk management processes by making sure that we manage our risks in the organisation well and being monitored and reported.	It's not my responsibility nor my role I am just assisting because there is no dedicated official for compliance and risk management. That on its own result in the function not being performed religiously because e there is no dedication function for risk because my responsibility is to just coordinate risk. Not necessarily that see to it that all the advices and	I am Deputy Director respons the implementation risk man department.
3	Access to resource	2	Do you have access to any ICT tools e.g. computer, system, internet etc?	Yes I do Laptop system (SAP) ms office, Outlook, N drive storage purposes. Smart phone. teams	Yes, I have access to the laptop, internet, cellphone, emails, teams, zoom and SAP GRC system	Yes do we have. I do have the laptop, the system we call SAP that we use to capture our risks. We access internet, emails, I can say we do have all the ICT Itools. And we do have teams.	Yes I have access to Computer, internet, ms teams, SAP GRC, email	Yes Ms Office, Ms Teams, laptop, smart phone
4	Usefulness	3	How do you use ICT tools in your daily risk management activities?	Laptop – MS office, risk registers, email/ cell phone communication, SAP – excel doc to conduct risk assessment, then update risk registers on pull up reports – all types of reports for various purposes, quarterly reports. Monitoring the status. SAP administrators, outstourced system. Risk owners, Risk champions and risk practitioners. RC assist the risk practictioners to update the system, are able to identify the risks through the system. System monitored by the risk practitioners.	Risk Management requires us to use IT system as we engage with different stakeholders like risk champions from regions and clusters. We capture information on the GRC system when we do risk assessments, I am also doing reporting on both word and the GRC system. When I am doing risk forums and any other meetings – I am using power point presentations as it makes it easy to engage my stakeholders through teams, During the Covid 19 period, I use of virtual meetings through Ms Teams. During this period we	With the laptop, everything we are capturing on the laptop. It's our working tool this one. And then even the system we are using it on the daily basis by going into that system whereby we capture our risk, retrieve the report. And everything that is needed in terms of our risks because it is a daily thing. And even the email, we communicate with the email more often We use internet even to access our system. The teams also is a daily thing, even now with this thing since even now we are faced with this thing of covid so for us to have meetings we are using teams. I can say we use them on daily basis. Having these ICT tools is very helpful.	That function of SAP GRC, the fact that it is centralised to national office it is delaying the process of submitting hence a person decide to submit on a method that is user friendly without having to go on the system because nayo its delaying me because it's not my responsibility	Ms Office – I use this packag activities in risk managemen assessment using exel, writir various stakeholders on wor presentations for those stake awareness purposes. I also u system for the assessment ar risks, drawing reports on the Ms Teams for conducting virt assessments, meetings and a engagements.
5	Impact of ICT resources	4	Is ICT playing an effective role in implementing risk management activities	I would not say effective but ICT is playing a role. Currently the assessment is done manually however the system is capable to do assessment. To avoid duplicate, preference woud be to do assessment on the system. The process that I found in the department, the system is still new, once we are comfortable with system we can do away with the manual process.	Yes The reason I am saying yes is that it makes things easy. We are able to connect with stakeholders through the network. Without ICT I was not going to be able to perform my duties.	What I can say is that it plays a major role, my answer is YES. In us for example, for us to work we need IT. Even with our system whereby we capture everything pertaining to our work. It becomes easy when it comes to reporting because we even receive the reports from that particular system unlike when using manual. The issue of the meetings, we do need cases where we need to go to meet in one room but with this ICT tool teams, it's easy to just log in on teams and we have our meeting. As risk management I can say meeting is a daily thing because we meet with various stakeholders so even if we don't talk to them via meetings, the email we get from ICT we are able to communicate via email and do what we want as risk management. So really ICT plays a major role in our activities, without it we may not survive.	No Department not funding the program ICT – risk of lack of funding in the regions. No progressiveness in technology. If the …IT investment in the department	Yes it does play an effective r It makes life easier especiall management. The reason why is at the moment we have Co having a laptop I am able to and having internet access I research from home on interr the risks register SAP while I also I am still able communi colleagues on Team. And als to do all risk management fu home. So having ICT is really

Appendix Q:Emerged Key themes

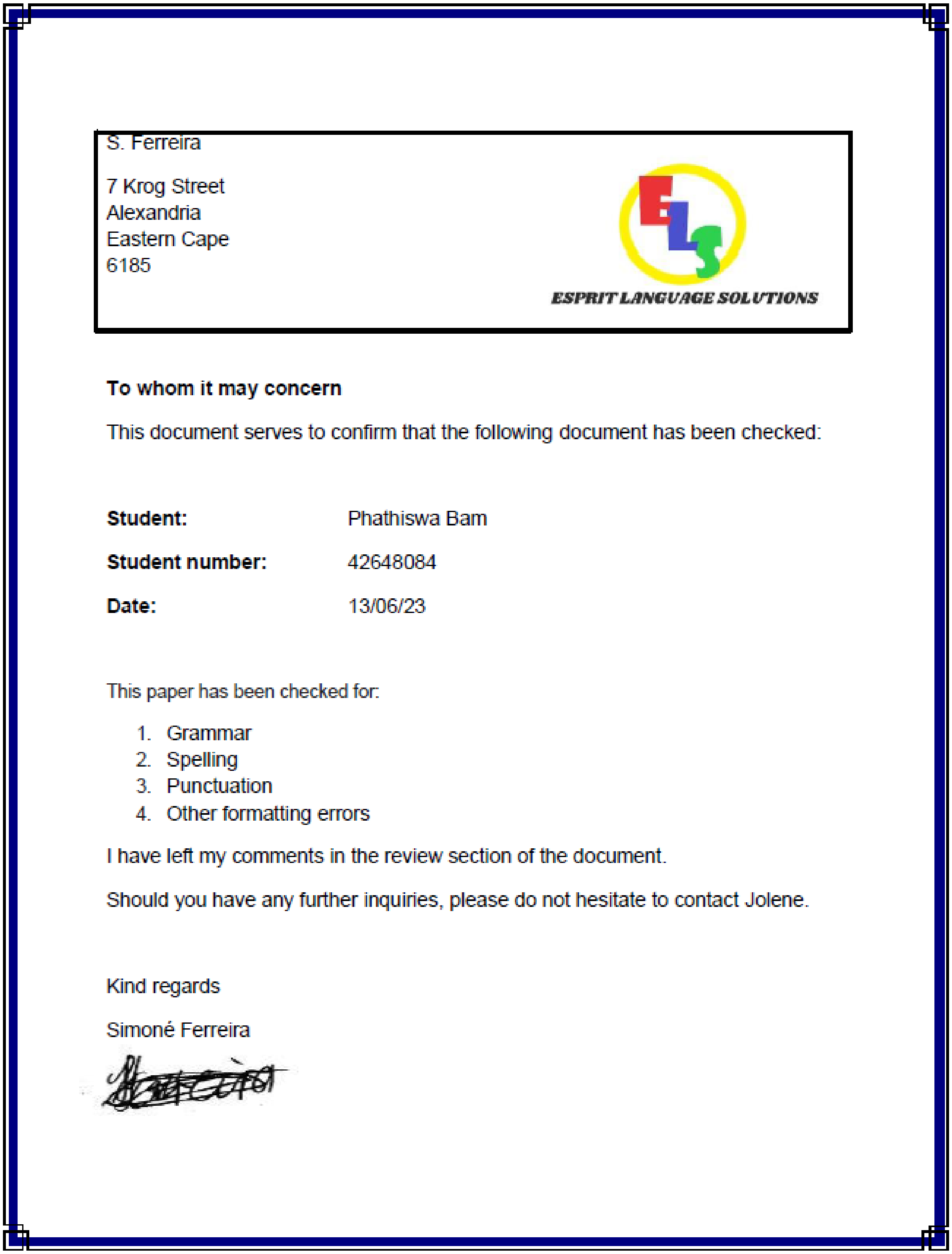


A	B	C
Access	**Impact**	**Usefulness**
Yes Laptop system (SAP) ms office, Outlook, N drive. Smart phone. Teams	ICT plays a major role RM effective role	Communicate, meetings, engagements, storage, awareness, assessments, reports **Covid 19 period**
IT System capabilities	Risk committees	Awareness
the system is capable to do assessment, update risk registers on pull up reports, System monitored by the risk practitioners	prepare for arranging logistics for the risk management committee, using power point presentations, teams, Meeting packs sent through outlook	awareness processes to instil the culture of risk management, risk forums, use IT as we engage with different stakeholders, For the implementation of Risk Appetite T videos were used

Themes

Supporting the themes

Appendix R: Language Editor's Letter



S. Ferreira

7 Krog Street
Alexandria
Eastern Cape
6185

ESPRIT LANGUAGE SOLUTIONS

To whom it may concern

This document serves to confirm that the following document has been checked:

Student:	Phathiswa Bam
Student number:	42648084
Date:	13/06/23

This paper has been checked for:

1. Grammar
2. Spelling
3. Punctuation
4. Other formatting errors

I have left my comments in the review section of the document.

Should you have any further inquiries, please do not hesitate to contact Jolene.

Kind regards

Simoné Ferreira