Cape Peninsula University of Technology

Effectiveness of risk management in the utilisation of mobile devices within local government entities in the Namakwa District, Northern Cape

by

PATRICK OTTO

Dissertation submitted in fulfillment of the requirements for the degree
Master of Internal Auditing

in the Faculty of Business and Management Sciences
at the Cape Peninsula University of Technology

Supervisor: Dr H. Benedict
Co-supervisor: Prof J. Dubihlela

Cape Town
October 2019

DECLARATION

I, Patrick Otto, declare that the contents of this dissertation represent my own unaided work, and that the dissertation has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed____________________________ Date 10/10/2020

ABSTRACT

This research focuses on the effectiveness of risk management in the utilisation of mobile devices in local government entities in the Namakwa District of the Northern Cape region. The introduction of mobile devices has resulted in offices not being the only place where business is conducted, as access to the enterprise's network is now possible with such devices. Employees have started to utilise mobile devices for business and personal use, which comes with potential risk exposure to organisations. Therefore, effective risk management practices are pivotal within such organisations. The aim of the study is to ascertain whether these organisations that permit the use of mobile device connections to their networks, are practising effective risk management, specifically pertaining to mitigation at an operational level. The research includes a literature review as well as an in-depth investigation to determine the effectiveness of risk management in the utilisation of mobile devices within these entities. A quantitative research method was applied in the study by obtaining responses from a sample of participants in the Namakwa District of the Northern Cape region, using closed-ended questions in the questionnaire, which provided the participants with a predetermined list of coded responses. The results were analysed and indicate that the majority of the respondents do utilise mobile devices in their organisations. In general, these entities make more use of laptops than any other types of mobile devices. The results indicate that these organisations also still apply the traditional approach of providing their employees with specifically approved types of mobile devices (corporate-owned device) and therefore do not support the Bring-Your-Own-Device or Choose-Your-Own-Device strategy. It was also found that these entities have implemented pockets of risk management practices; however, there is a clear indication from the results that more efforts are required to ensure improvement, specifically in terms of mitigation at an operational level.

ACKNOWLEDGEMENTS

I wish to thank:

- Dr H. Benedict and Prof J. Dubihlela for their support and guidance received;
- Cheryl Thomson for her professional editing; and
- My family for their continuous support.

DEDICATION

I would like to dedicate this research study to the entire Otto family, for all their support and encouragement received.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

AC	Audit Committee
BYOD	Bring-Your-Own-Device
CAE	Chief Audit Executive
COSO	Committee on Sponsoring Organisations
COPED	Corporate owned personally enabled device
CYOD	Choose-Your-Own-Device
ERP	Enterprise Resource Planning
IAP	Internal Audit Plan
IIA	Institute of Internal Auditors
MDM	Mobile Device Management
MFMA	Municipal Finance Management Act
PERM	Perceived E-Readiness Model
RMC	Risk Management Committee
SALGA	South African Local Government Association
VPN	Virtual Private Network

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

Figure 1.1 graphically presents the logical flow of this dissertation.

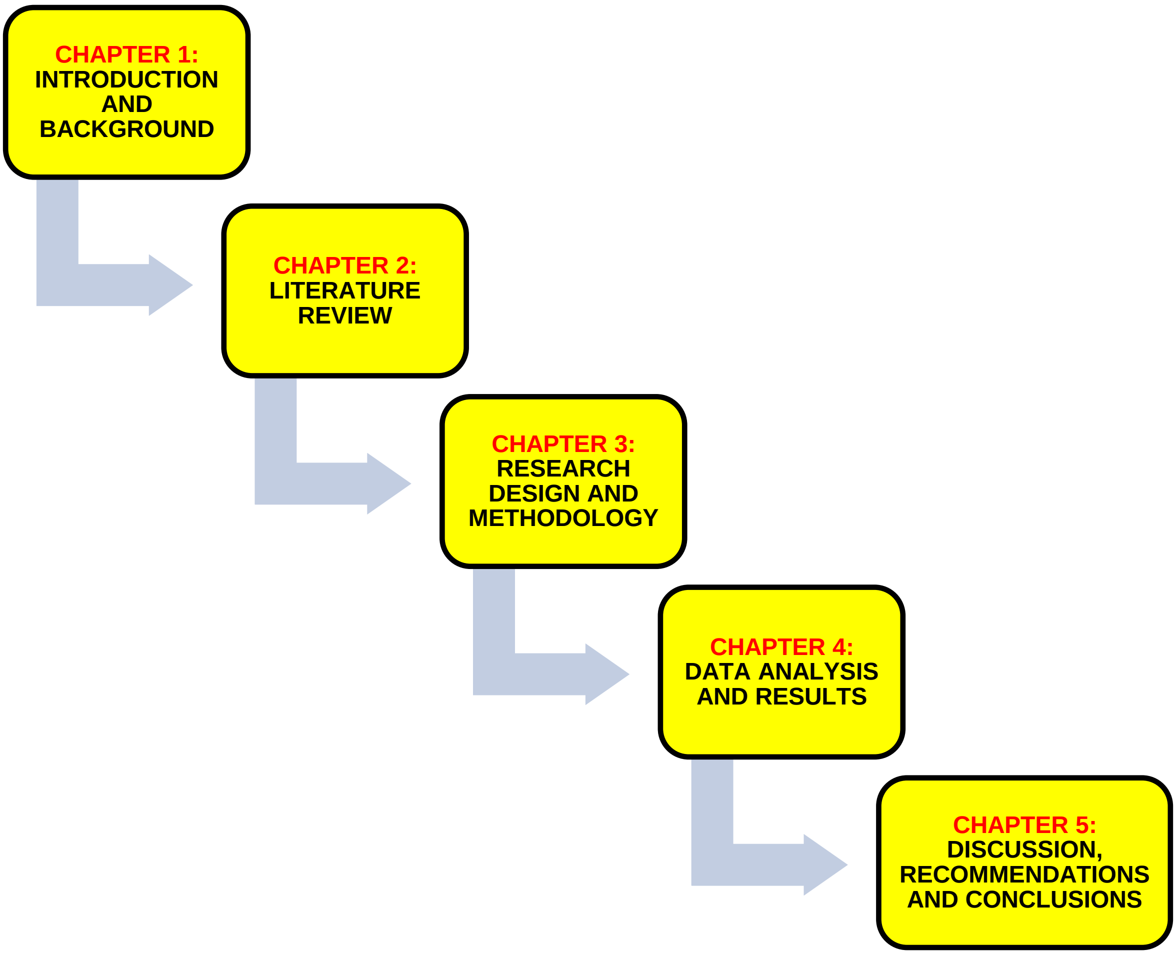

CHAPTER 1:
INTRODUCTION AND BACKGROUND
CHAPTER 2:
LITERATURE REVIEW
CHAPTER 3:
RESEARCH DESIGN AND METHODOLOGY
CHAPTER 4:
DATA ANALYSIS AND RESULTS
CHAPTER 5:
DISCUSSION, RECOMMENDATIONS AND CONCLUSIONS

Figure 1.1: Research project layout

Chapter One introduces the study and gives a background of the research performed. Figure 1.2 below outlines the flow of Chapter One.

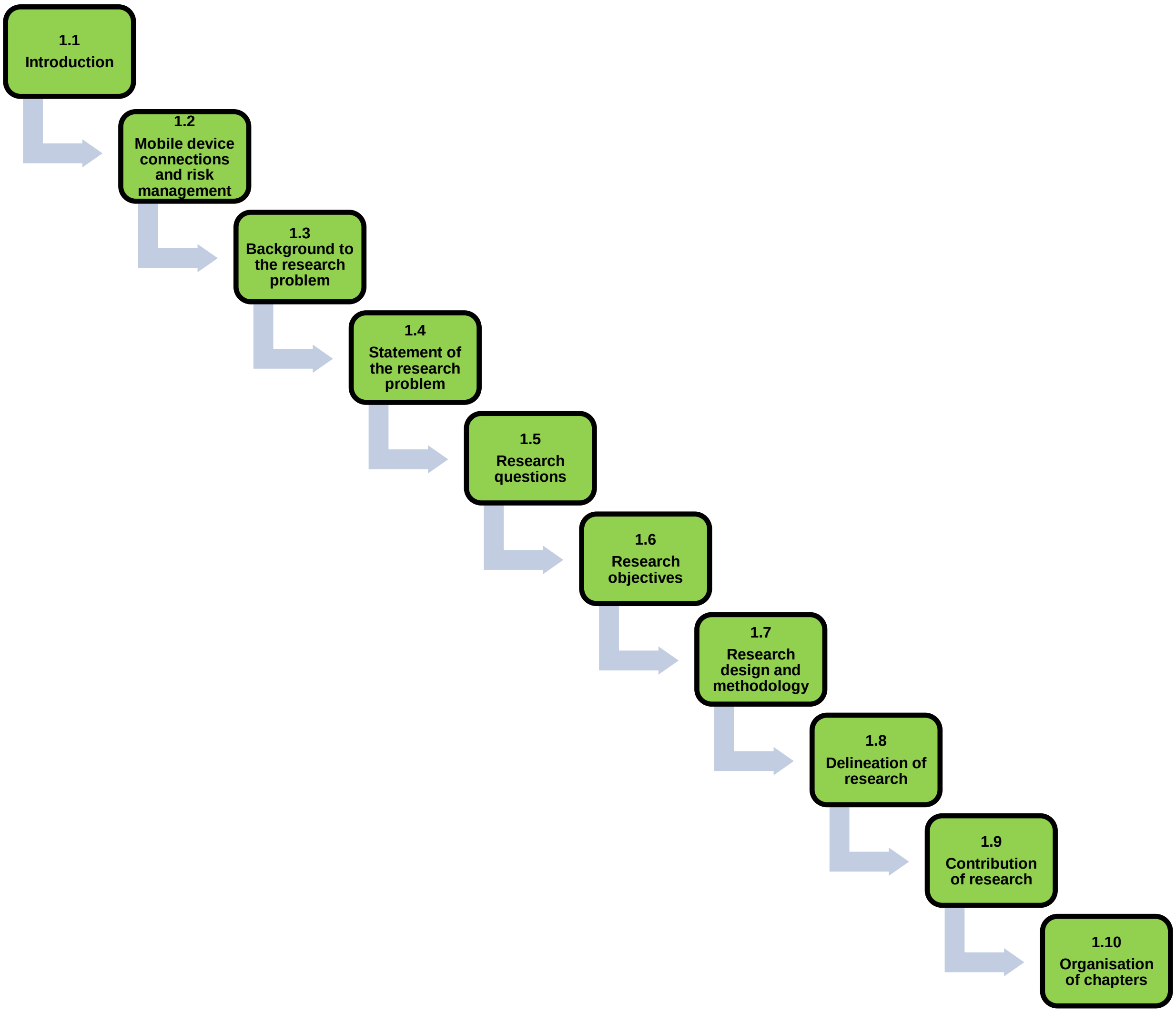


Figure 1.2: Layout of Chapter One

1.2 Mobile device connections and risk management

Since the introduction of mobile devices (tablets and smartphones) in recent years, user expectations and needs have gradually grown from the need to make a telephone call and sending a short text message with these devices during communication, to the requirements such as being able to connect wirelessly to networks. Therefore, it was ultimately going to enter the workspace. Growth in terms of the capabilities of these devices enabled them to access networks and information such as e-mails and viewing documents to name a few, according to Mowafi *et al*. (2015). This extended the area relating to their use, over and above the already used laptops. According to Jamaluddin, Ahmad, Alias and Simun (2015), entities soon realise potential benefits in using smart devices, such as employees being able to access organisational information whilst not in the office, which could increase productivity. This view is supported by Sheldon (2013b), who is of the opinion that mobile devices assist employees in performing their duties more efficiently and productively. According to Ludwig (2018), research has shown that using mobile devices positively impacting productivity. Treleaven (2014) reports that there is growth in use of these devices (in support of employees) within workplaces. However, Chen and Li (2017) state that information is at risk of being compromised where such users are unable to secure their devices.

A concern relating to the introduction of mobile devices in the workplace is the ethical implications relating to its use. Working from anywhere results in privacy issues since the individual is reachable anytime during the day. Possibility of distractions whilst driving because of engaging in business calls and the use of it for non-work-related activities (private calls), is an ethical concern relating to this technology (Kelley, n.d.). The accessing of online activities (social media networks) during working hours is another associated ethical dilemma (Kim, 2018).

Therefore, the use of mobile devices within organisations could have an impact on the entity's risks. An adequate and effective risk management process is pivotal in ensuring an acceptable residual risk exposure to the organisation.

1.3 Background to the research problem

Whilst reviewing available literature on the topic of "mobile device connections to an enterprise's network", it became evident that organisations note that there are potential advantages in utilising these devices on their business networks. These advantages include an increase in efficiency and productivity. However, they also noted possible concerns and risks of this strategy as well as the importance of managing it.

Organisations permit employees to utilise mobile devices at their workspace (Vignesh & Asha, 2015). However, the approach to use mobile devices has several negatives, which include the leakage of critical and sensitive corporate information *(*Bann, Singh & Samsudin, 2015*)*. Past research confirms that mobile device use currently tops the security risk list *(*Kleiner & Disterer, 2015*)*. According to Disterer and Kleiner (2013), employees started to synchronize mobile device use for business and personal use because logistically it was easier. Therefore, instead of carrying multiple devices, the user only carries one. However, this approach presents opportunities as well as potential risks. This is mentioned by Loose, Weeger and Gewald (2013), raising the question of whether the use of employees' private devices within the organisation outweigh cost and risk.

An important consideration by Souppaya and Scarfone (2013) relates to the development and implementation of a policy to guide users within such a strategy. A policy provides information on the process to follow (in the event of a lost device). Therefore, education of users is very important.

The use of employee-owned mobile devices, known as the Bring-Your-Own-Device (BYOD) strategy is very appealing in cost saving for organisations, but security relating to such an approach should be of utmost importance (Banerjee & Wallace, 2014). Since this approach blurs the lines between privacy and business, security should be seriously considered. According to Harris, Patten and Regan (2013), the management of mobile device security is still a work in progress, supported by the fact that a recent study indicated that 68% of organisations utilising the use of these devices, struggle to identify vulnerabilities resulting from mobile device connections to their network. Results further indicate that adequate mitigation is lacking and therefore results in risk exposure to the organisation (Harris *et al.*, 2013). This conclusion indicates that security of BYOD remains to be addressed, supported by Shim, Mittleman, Welke, French and Guo (2013) who claim that one of the main reasons is the aversion to amending security protocols.

This change in corporate culture over the last decade to accommodate smart devices comes with great benefits. Despite such benefits, it should be noted that it also expands the risk of data being compromised (van Kessel, Layman, Blackmore, Burnet & Harada, 2013), and therefore forces security to be well thought through on dealing with risks of uncontrolled devices on the enterprise's network(s) (Cardinal, 2016). The main contributor to this risk materialising is security awareness lagging behind (van Kessel *et al.*, 2013).

According to Souppaya and Scarfone (2013), security objectives (integrity, confidentiality and availability) can be achieved through securing of mobile devices against threats. A further enhancement in the achievement of such objectives includes the security awareness and training of users to educate them properly (Harris *et al.*, 2013) and having a sound policy (Siddiqui, 2014).

Since most organisations exist to provide value for investors and/or stakeholders but are facing challenges and uncertainties in achieving such, as explained by Steinberg, Martens, Everson and Nottingham (2004:3) in the COSO Enterprise Risk

Management Framework. These challenges and/or uncertainties are better known as risks and opportunities in the corporate environment. According to the framework, such risks and opportunities can either erode or improve the achievement of an organisation's objectives and therefore need to be dealt with and managed. It should be noted that the management of risk improves the likelihood of organisational objectives being achieved. Tupa, Simota and Frantisek (2017) allude to this, that in the current economic environment, a working management strategy should include, amongst others, an effective risk management process. This process includes actions such as understanding what the risk is, the current mitigation in place and an assessment to establish whether such mitigation is adequate (Dubihlela & Nqala, 2017). Where this mitigation is inadequate, additional actions are required to drive such exposure down to a level accepted in terms of the organisational risk appetite.

Organisations utilise various tools to support and improve risk management activities. Information gathered and discussed during the process of risk management (what the risk is, what the likelihood of it occurring is, what the potential impact is, what current mitigation is in place) are recorded in the tool. According to Tsiga, Emes and Smith (2017) the use of such tools enable the performance of an analysis on a cluster of risks as well as a specific risk. This also enables the organisation to monitor inherent and residual risk exposure to the business on an ongoing basis.

Therefore, risk management is not a stagnant process; hence, organisations are required to review it constantly, thereby ensuring that organisations manage their risks by having adequate and effective mitigation in place for risks relevant to the business.

The government structures within South Africa are in three (3) spheres; namely National, Provincial and Local government (The Constitution of the Republic of South Africa, 1996). The government sphere, specifically relating to Local Government, is a make-up of Municipalities in accordance with Chapter Seven (7) of the Constitution. Municipalities are responsible for managing their administration, planning and budgeting processes in such a way that they deliver basic needs (services) as well as promote social and economic development within their communities (The Constitution of the Republic of South Africa, 1996). The structures of municipalities within South Africa is further divided into three (3) categories; namely, Category A (metropolitan municipalities), Category B (Local Municipalities) and Category C (District Municipalities) (The Constitution of the Republic of South Africa, 1996).

According to an online overview of the research focus area (Municipalities of South Africa, 2020: online), the Namakwa District consist of seven (7) entities; one (1) District Municipality and six (6) Local Municipalities.

Furthermore, considering the usage of mobile devices by employees within these municipalities in the Namakwa District during their day-to-day activities, an increased probability exist on the associated risk exposures materialising. Therefore, risk management is fundamental within these entities, and could not be overemphasised.

1.4 Statement of research problem

Mobile device use became important in the modern business world. However, it comes with risks, such as data compromise as previously discussed. This could cause serious harm to an organisation.

Therefore, since the introduction of mobile devices into organisations poses potential risks to the business, an effective risk management process within an entity is of utmost importance.

This research focuses on ascertaining whether in such cases where mobile devices are utilised in local government entities located in the Namakwa District of the Northern Cape; whether adequate and effective risk management processes exist and are practised.

1.5 Research questions

1.5.1 Main research question

The key question of the research is to ascertain if the connection of mobile devices in local government entities located in the Namakwa District of the Northern Cape, enhance efficiency and productivity, whilst the organisation ensures that the related risks are managed within its appetite of risk exposure.

1.5.2 Research sub-questions

The research sub-questions are:

i) Does management of local government entities in the Namakwa District of the Northern Cape, deem mobility of employees (connections with a mobile device to the entity’s computer network) as important to achieve organisational objectives.

ii) Does employees of local government entities in the Namakwa District of the Northern Cape, deem connections with mobile devices to the entity's computer network(s) as necessary to deliver on organisational objectives.

iii) Does the risk exposure increase in instances where mobile device connections to the local government entities in the Namakwa District are permitted.

iv) Is risk management effectively performed in instances where mobile device connections to the network of local government entities in the Namakwa District are allowed?

1.6 Research objectives

1.6.1 Main objectives

i) To understand the importance of mobility to management and employees of local government entities in the Namakwa District of the Northern Cape, in achievement of organisational objectives; and

ii) To understand the effectiveness of risk management where mobile device connections to local government networks are permitted within the Namakwa District of the Northern Cape.

1.7 Research design and methodology

1.7.1 Research approach

A study could apply either a quantitative or qualitative approach (Collis & Hussey, 2014:5-6).

The research seeks to establish the view of different employees within local government entities located in the Namakwa District during this study to answer the research objectives previously explained in Section 1.6.1. Therefore, the quantitative research approach is followed during the study.

1.7.2 Research method

A quantitative research method was followed, whereby a research questionnaire was administered to a sample of participants employed within the local government entities located in the Namakwa District. This research questionnaire included a number of closed questions with a predetermined list of responses that were coded in advance. The respondent made a selection from this list provided (Greenfield & Greener, 2016:206). Information obtained from the completed research questionnaires were recorded in a Microsoft Excel template and analysed using the Statistical Package for Social Sciences (SPSS) software. Inferential as well as Descriptive Statistics were performed.

Further information relating to the research design and methodology is explained in Chapter Three.

1.8 Delineation of the research

The research focuses on local government entities located within the Namakwa District area. Therefore, the study were limited to municipalities in the Namakwa District within the Northern Cape, South Africa. The Namakwa District comprises of seven entities, which includes one District Municipality and six Local Municipalities. No other organisations were included in this study.

1.9 Contribution of the research

The significance of this study to organisations is an enhanced understanding of:

i) Whether management and employees deem the use of mobile devices as important in achieving organisational objectives within local government; and

ii) Whether risk management process is adequate and effective in instances where mobile device connection is allowed in local government entities' network(s).

The benefits to society of this study are:

i) Improving awareness pertaining to exposure relating to the use of mobile devices in our daily lives/interactions;

ii) Re-iterating the importance of not only the safeguarding of the actual asset, but also the information stored on the device; and

iii) Educating the users on possible mitigation to be implemented to minimise the possibility of exposure(s) materialising, which come with the use of these devices.

The research concludes with recommendations relating to possible improvements in the risk management process of the use of mobile devices within local government entities in the Namakwa District area.

1.10 Organisation of chapters

The research project is organised as follows.

Chapter One: Introduction

Chapter One introduces the study and gives a background to the research.

Chapter Two: Literature review

This chapter offers insights into the literature of previous research in the area on the topic of this study, by surveying books and peer reviewed scholar articles to make mention of a few techniques used. This provides an understanding of information submitted by other researchers in the specific field and provides context relating to the research problem.

Chapter Three: Research design and methodology

This chapter discusses information on the research methodology and design followed. This includes information on the research approach, population within the study and sampling procedures. The information relating to the data collection process utilising a research questionnaire as a data collection tool is also explained. Ethical considerations of the study are clarified within this chapter.

Chapter Four: Data analysis and results

This chapter offers insights relating to the data analysis and results of the study. This includes information relating to the methodology of the analyses applied, validation of data received back from respondents and formatting of such data to mention a few. The summary of results emanating from this analysis is also discussed here.

Chapter Five: Discussion, recommendations and conclusions

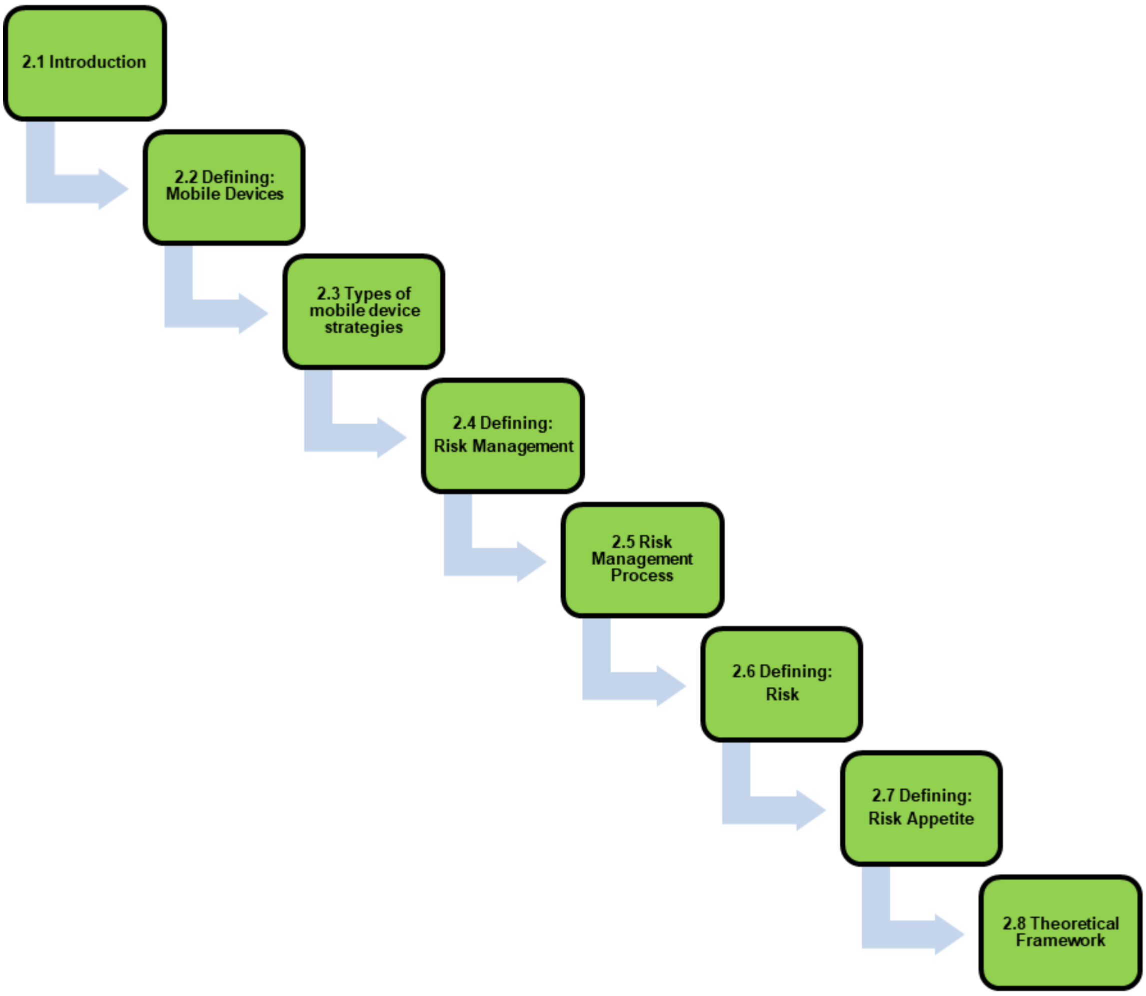
This chapter discusses information relating to conclusions drawn from the research results and analysis performed on collected data within this study, as well as the related findings and recommendations relating to further studies that could be endeavoured upon associated with this research.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The previous chapter introduced the reader to the study, explaining the research problem, research objectives and the research questions. This chapter offers insight into literature of previous research on mobile device use. It further provides an understanding of information submitted by other researchers in this field and gives context relating to this research performed. Another objective is to describe the critical concepts utilised within the study for ease of reference and avoiding of confusion. The theoretical framework discussed in the study provides an explanation on theories utilised in the research.

The layout of Chapter Two is illustrated below.


2.1 Introduction
2.2 Defining: Mobile Devices
2.3 Types of mobile device strategies
2.4 Defining: Risk Management
2.5 Risk Management Process
2.6 Defining: Risk
2.7 Defining: Risk Appetite
2.8 Theoretical Framework

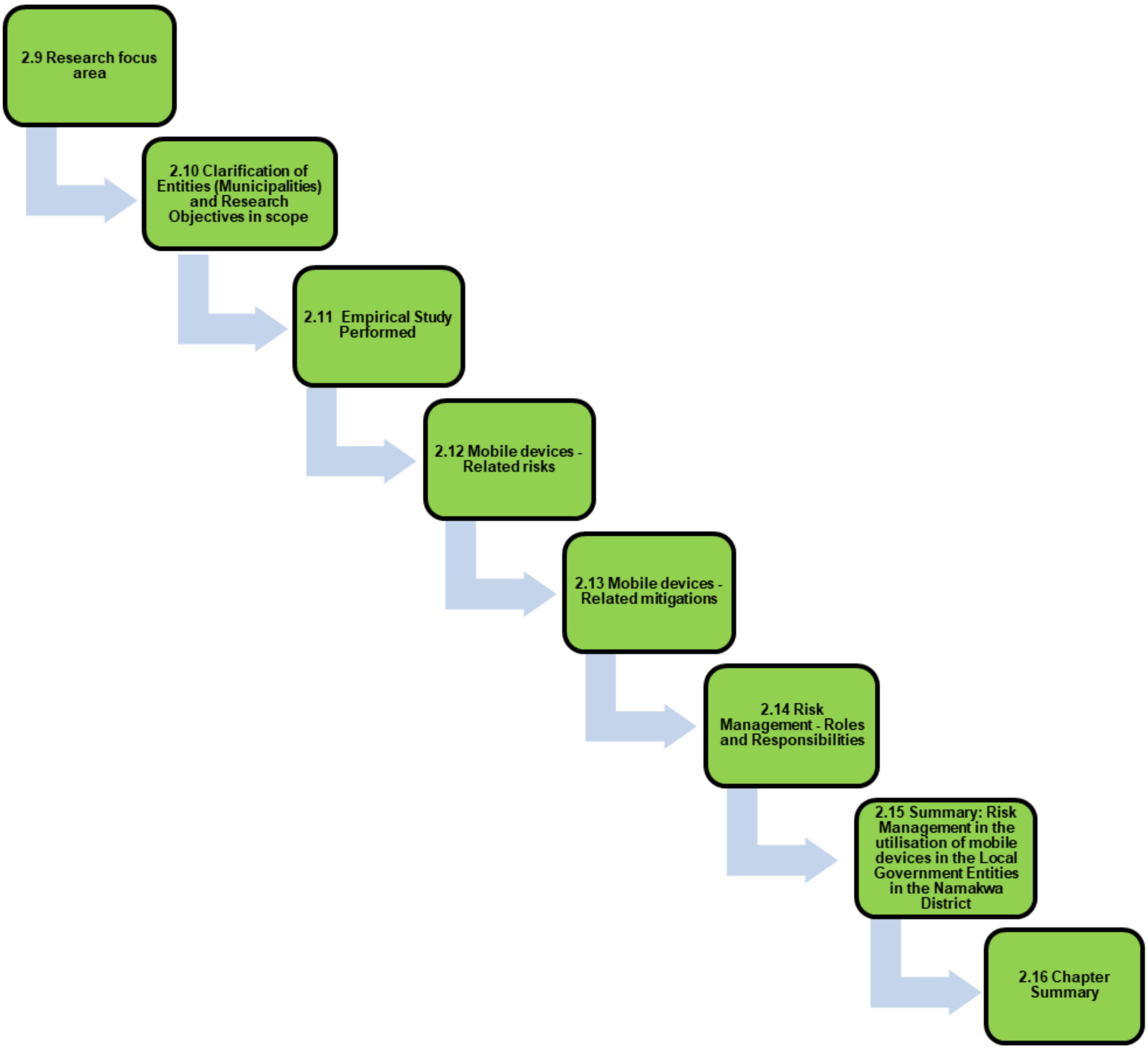

2.9 Research focus area
2.10 Clarification of Entities (Municipalities) and Research Objectives in scope
2.11 Empirical Study Performed
2.12 Mobile devices - Related risks
2.13 Mobile devices - Related mitigations
2.14 Risk Management - Roles and Responsibilities
2.15 Summary: Risk Management in the utilisation of mobile devices in the Local Government Entities in the Namakwa District
2.16 Chapter Summary

Figure 2.1: Layout of Chapter Two

2.2 Defining mobile devices

According to Sahd and Rudman (2016), mobile devices can be defined as computing devices that possesses storing of information as well as communication abilities, which could also be utilised to access information remotely.

These devices include items such as smartphones, laptops and tablets, which were explained in sections 2.2.1 to 2.2.3 and are illustrated in Figure 2.2 below.

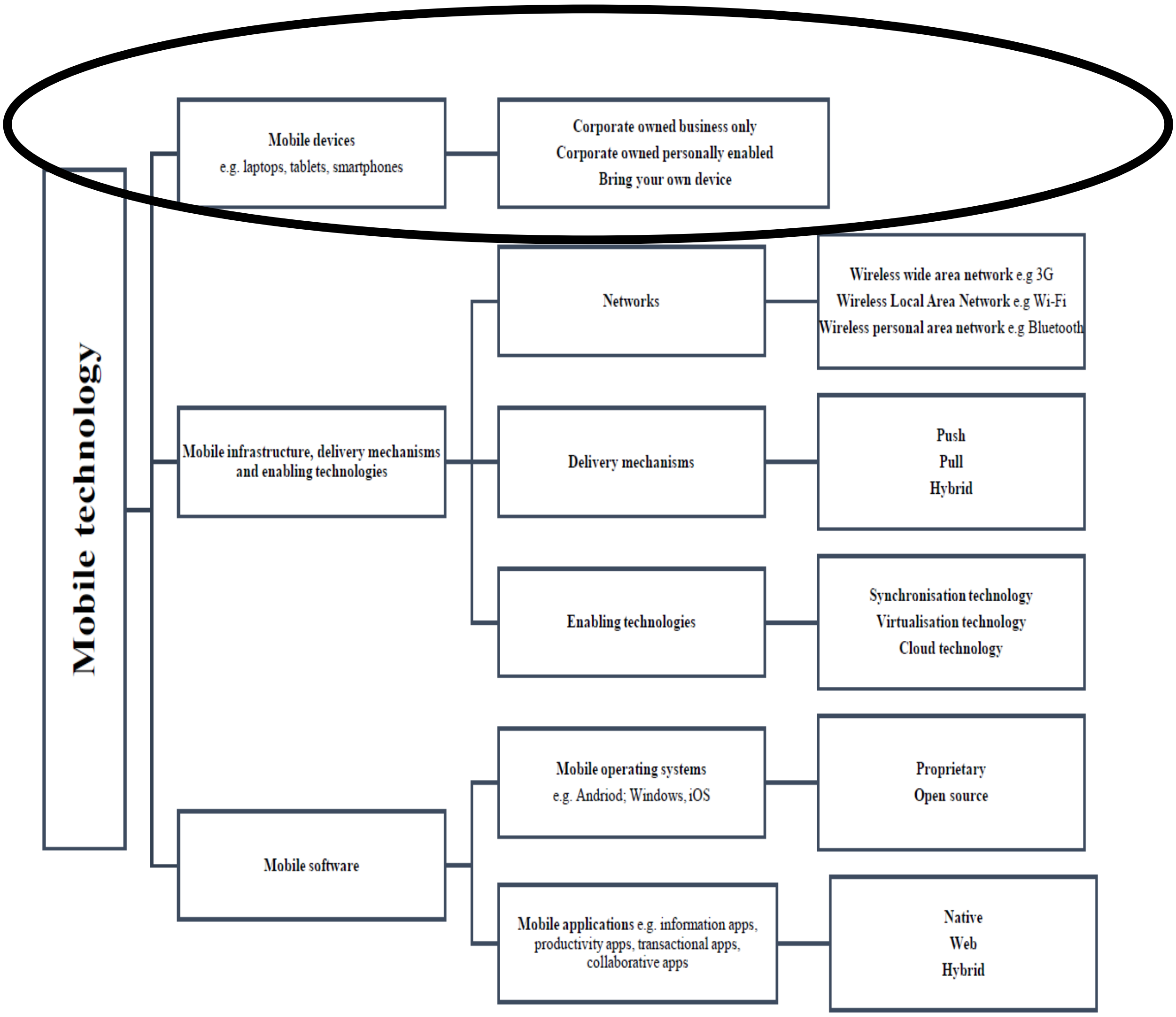

Mobile technology
Mobile devices
e.g. laptops, tablets, smartphones
Corporate owned business only
Corporate owned personally enabled
Bring your own device
Networks
Wireless wide area network e.g 3G
Wireless Local Area Network e.g Wi-Fi
Wireless personal area network e.g Bluetooth
Mobile infrastructure, delivery mechanisms and enabling technologies
Delivery mechanisms
Push
Pull
Hybrid
Enabling technologies
Synchronisation technology
Virtualisation technology
Cloud technology
Mobile operating systems
e.g. Andriod; Windows, iOS
Proprietary
Open source
Mobile software
Mobile applications e.g. information apps, productivity apps, transactional apps, collaborative apps
Native
Web
Hybrid

Figure 2.2: Components of the mobile technology solution

Source: Sahd and Rudman (2016:1081)

2.2.1 Smartphones

Hornby (2010:1404) explains the term “smartphone” as a mobile phone or device which has certain abilities and functionalities of a computer.

This is confirmed by McIntosh (2015:1468), who explains that a smartphone can also be defined as a mobile phone which can be utilised as a computer and has the functionality to connect to the Internet.

Smartphone refers to a handheld device that has the ability to perform advanced computing tasks like e-commerce, Internet communication and retrieving information, just to mention of a few of its capabilities (Miakotko, n.d.).

2.2.2 Laptops

Laptops are considered portable computer devices that are convenient for use by an individual whilst travelling, as explained by Allen (1990:666).

According to Hornby (2010:836), a laptop is a computer that is mobile in nature, and is easy to carry around by the user. This is further confirmed by Smith (2014:283), indicating that a laptop is also referred to as a portable computer and therefore is convenient for use.

2.2.3 Tablets

Hornby (2010:1518) explains that a tablet is a small computer that is mobile in nature, has a touch screen and is easily carried around by users. It is also noted by Smith (2014:499), who opines that a tablet is a moveable small computer, has a touch screen and is very convenient to use.

McIntosh (2015:1598) confirms that a tablet is a flat, small computer device that does not have a keyboard but is equipped with a touch screen for user operation.

2.3 Types of mobile device strategies

Organisations that envisage the utilisation of mobile devices could consider the implementation of one or a combination of the following approaches, as illustrated in Figure 2.3 below.

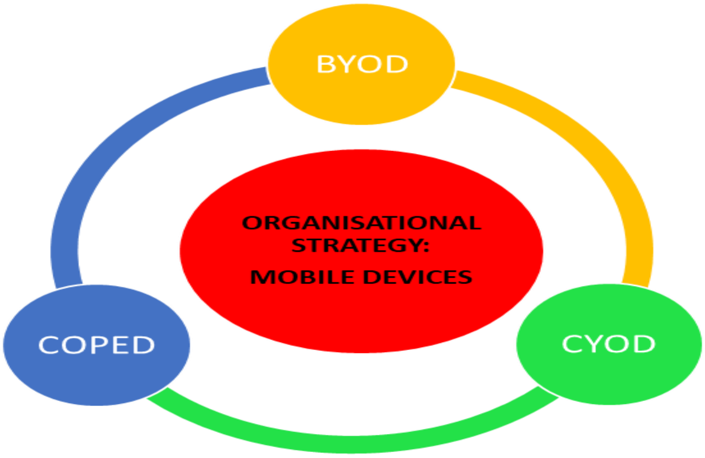


Figure 2.3: Different strategies available

Source: Akram, Markantonakis and Holloway (n.d.:3)

2.3.1 Bring-Your-Own-Device

Entities permitting personnel to make use of their personal mobile devices for business activities (BYOD), is a strategy commonly applied during recent years. Schwartz (2015) and Gaff (2015) also confirm that BYOD refers to the approach where workers are permitted to make use of their personal mobile devices in the workplace. According to Pereira, Barreto and Amaral (2017) the BYOD tendency is one of the new organisational technology changes within business in recent times. This view is supported by Eslahi, Nesiri Hashim, Tahir and Saad (2013) who indicate that this approach brought convenience and flexibility for users.

According to Musarurwa and Flowerday (2018), BYOD became important in the implementation of organisational strategy, however information security remains to be a challenge.

Twinomurinzi and Mawela (2014) is of the opinion that strong awareness exist amongst employees within South African organisations, pertaining to BYOD; however employers are still hesitant to formally utilise such a strategy. This was further confirmed by Ruxwana and Msibi (2018), indicating low readiness levels within South Africa, specifically attributed to technological and organisational factors. Another opinion by Gustav and Kabanda (2016), indicate that although the use of BYOD is happening in the South African financial sector, it was not formally addopted.

Therefore, considering the information privacy challenges where organisations opt to utilise the BYOD stategy; Musarurwa and Flowerday (2019) proposed an information privacy framework in order to govern such risks. This framework focusses on the three pillars, namely Organisation (environment and governance), Individual (attitude, habit and knowledge) and Technology (mobile device management).

2.3.2 Corporate owned personally enabled device

Whilst the BYOD strategy entails the use of the employee’s personally owned mobile device for business purposes; the corporate owned, personally enabled device (COPED) strategy refers to the organisation purchasing the device and therefore owning it (Sheldon, 2013a). In such an instance, the employee is allowed to also make use of the device for personal use (Sheldon, 2013a). This is confirmed by Porro (2014), revealing that the COPED strategy refers to the employees being provided with an organisationally-approved device.

2.3.3 Choose-Your-Own-Device

Another available strategy that could be considered, as explained by Akram, Markantonakis and Holloway (2016) and Tairov (2016), is the Choose Your Own Device (CYOD) strategy, which entails the organisation providing the user with a list of pre-approved devices that could be obtained by the user, which will be allowed by the entity to connect to their network. Schwartz (2015) confirms that CYOD refer to the approach where employees are provided with a mobile device by their employers. This strategy provides some comfort to the organisation in the sense that the entity could perform pre-configuration of their systems, in line with the security requirements needed. According to Maggie (2015), entities would rather allow the CYOD strategy because then the organisation installs their own security software and can alter the settings of the device to improve control, which is important. However, Weldon (2014) is of the opinion that irrespective of entities embracing a specific approach (BYOD or CYOD), the risk associated with security and privacy is ultimately the same and therefore the important fact is "what an entity does to secure organisational information". Table 2.1 provides a comparison between the three options or strategies available when considering the use of smart devices within organisations.

Table 2.1: Comparison between different strategies available

CRITERIA	COPED	BYOD	CYOD
Ownership of Device	Company (Informarion Technology Department)	Employee (User)	Enterprise's Agreed/Pre-configured
Application Control	Full (Informarion Technology Department)	Full (User)	Partial (Informarion Technology Department and User)
Company Asset Protection	Full (Informarion Technology Department)	Partial (User)	Partial (Informarion Technology Department and User)
Responsible – Security of Device	Informarion Technology Department	User	Partial (IT Department and User)
Privacy Issues of Operator	Substantial	Restricted	Restricted
Freedom for employee use	Restricted	Full	Restricted

Source: Akram *et al*. (2016:3)

2.4 Defining risk management

Risk management is defined by Steinberg *et al.* (2004:16) as:

> A practice implemented by an establishment's leadership, which is applied during strategy setting and operations; identifying and managing possible events which could hinder the organisation from achieving predetermined objectives and therefore improving the possibility of such objectives being achieved.

A further explanation of the term "risk management" comes from Valsamakis, Vivian and du Toit (2005:12), describing it as a management role that targets the securing of an entity's assets and resources against consequences of risk, by implementing related mitigation within the organisation. Therefore, the associated risks as discussed in section 2.12 (user privacy risks, physical security risks, organisation and user information security risks and compliance risks), are required to be managed. Hence, it is included in the process, where it is subjected to an assessment to ascertain the inherent risk exposure (Dubihlela & Nqala, 2017). Dependent on the inherent risk exposure in accordance with the business' risk strategy and appetite, mitigation will be considered to decrease the exposure to a level where the organisation is willing to accept it.

Mitigation is generally referred to as a control within the corporate environment. A control is an action taken by the board (directors) and management in the process of managing risks relevant to the business, thereby increasing the likelihood of predetermined goals being achieved (Spencer Pickett, 2005a:99).

The COSO framework (internal control) as shown in Figure 2.4 below, is a good illustration.

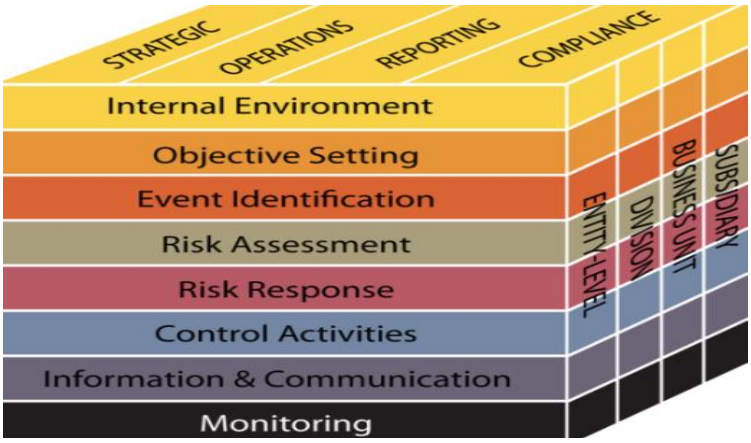


Figure 2.4: COSO internal control framework

Source: Steinberg *et al.* (2004)

2.5 Risk management process

Fraser and Simkins (2010:106-110) report that the following information and steps relate to the risk management process:

Step 1 - Identification of risk:
Identification and logging of risks associated with the process in a risk register.

According to Kielbus and Karpisz (2019), the risk management process is a critical part of any planning process, as it identify threats associated with applicable organisational objectives. This sentiment was shared by Tonmoy, Rissik and Palutikof (2019), agreeing that conducting risk workshops with appropriate stakeholders to identify relevant risks is imperative. Tiganoaia, Niculescu, Negoita and Popescu (2019) also confirmed the importance of the identification of all significant risks faced by an organisation, in an aid to achieve their objectives.

Step 2 – Analysing identified risk:
Understanding the risk to make knowledgeable decisions on treating it.

According to Jansen van Vuuren, Reyers and Van Schalkwyk (2017), the identification of a risk is merely the first step in the process, whereafter a measurement should be performed to establish the threat faced by the organisation. Importance with regard to the assessment of identified risks was also emphasised by Van der Poll and Mthiyane (2018). Bruwer and Siwangaza (2016) opines that the assessment of an identified risk should consider the potential likelihood of the risk occurance, as well as the potential impact, in case it realise.

Step 3 – Treatment of risk:
Identified risks are treated by applying a selected control.

According to Hopkin (2010:39), responding to risks could include options such as tolerating, treating, transferring or terminating it. This sentiment aligns with Steinberg *et al.* (2004:55), claiming that after identification and assessment of risks, management should determine an appropriate risk response, which could include:

- *Risk avoidance* – Exiting/avoiding activities introducing the risk;
- *Risk sharing* – Decreasing the probability and/or impact of the exposure by sharing it with a third party;
- *Risk acceptance* – Taking no action on the risk and therefore accepting it; and
- *Risk reduction* – Reducing the possibility, impact or both, regarding the exposure by putting mitigation in place.

Kielbus and Karpisz (2019) opines that the development of plans in an aid to avert or decrease the consequences of identified risks is important. This sentiment was shared by Tiganoaia *et al.* (2019), agreeing that treatment of identified risks is indeed necessary in the achievement of organisational goals (Dubihlela & Nqala, 2017).

Step 4 – Monitoring and review:

The monitoring and review is pivotal in the continuous improvement of the process as it looks at, amongst others, whether risks have changed, whether controls are working as intended and whether any new risks have evolved.

According to Aven (2015); monitoring is a way in which we may avoid events from occurring, as actions can be adjusted based on results obtained. Vasvari (2015) opines that the monitoring process is very important, as it enable the development of a more efficient risk management system.

Step 5 – Communication of results:

Results are communicated to relevant stakeholders.

According to Vasvari (2015); communication to the relevant stakeholders is important and contribute significantly in the decision making process.

The information as explained above is illustrated in Figure 2.5 below:

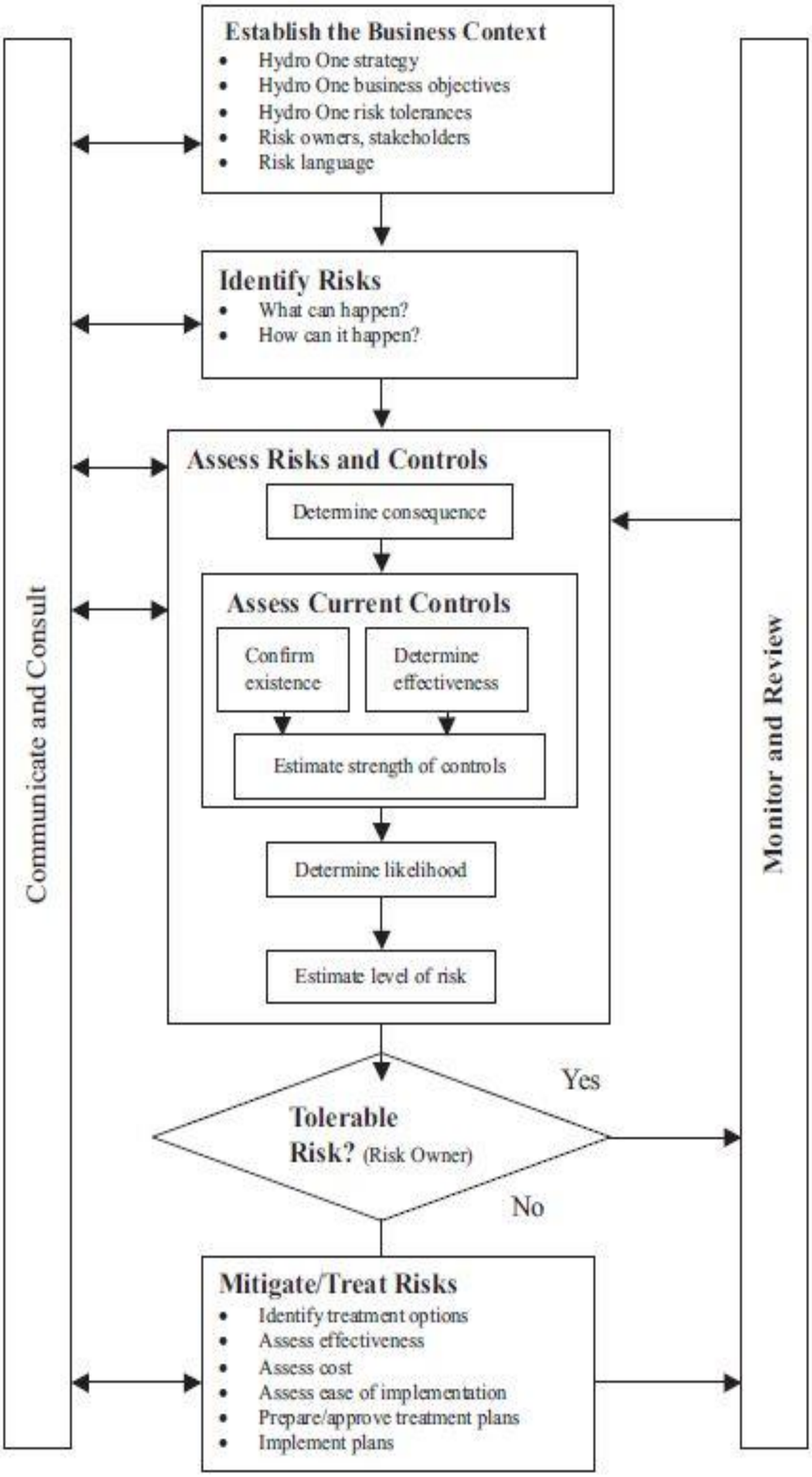


Figure 2.5: Risk management process

Source: Fraser & Simkins (2010:537)

2.6 Defining risk

According to Steinberg *et al.* (2004:16), risk is defined as all events that could occur which would undesirably impact the realisation of a business' goals. Hence, the realisation of the risk will negatively impact the possibility of the pre-determined organisational objectives being accomplished.

A further explanation of the term "risk" is provided by Valsamakis *et al.* (2005:27), as a deviation of the real result from the anticipated result. Therefore, it indicates the existence of uncertainty, which could impact the achievement of objectives.

Aven (2015) explains risk as:

- Probability of an unfortunate incident happening;
- Possibility of undesirable events occurring;
- Exposure to an organisation; and
- The result of an event linked to an uncertainty.

Another view relating to risk is the variation between the actual and expected results (Valsamakis, Vivian & du Toit, 2010:29). Horcher (2005:1) opines that risk is the chance of incurring losses during a process. It should be noted that risk is present in all projects, as a risk-free project is considered not worth chasing (Chapman & Ward, 2003). Therefore, risk is considered an important component influencing decision making. This was further clarified by Spencer Pickett (2005a:7), as being the possibility of an unwanted occurrence, such as impeding set organisational objectives from being achieved.

Risks relating to an organisation or entity are:

- Strategic risk; and
- Operational risk.

2.6.1 Strategic risk

Fraser and Simkins (2010:36) opine that a strategic risk relates to the performance of the organisational strategy in the event of something going wrong.

According to Hull (2015:574), strategic risk relates to an organisation's strategy and the assumptions associated with that specific strategy. Therefore, strategic risk refers to how bad the strategy will be performing in cases of deviations or something going wrong.

2.6.2 Operational risk

Operational risk is explained by Gregoriou (2007:1) as exposure to poor or unsuccessful internal business practices, people and structures. According to Christoffersen (2012:7), operational risk is the exposure pertaining to procedural failure and people making mistakes during operational processes.

It was further confirmed by Olsson (2002:35) that operational risks refer to the loss resulting from human actions, operational processes and technology, to name a few, which have an impact on an organisation's operations.

The level within the risk management framework model where strategic risk and operational risk are focused, is shown in Figure 2.6 below.

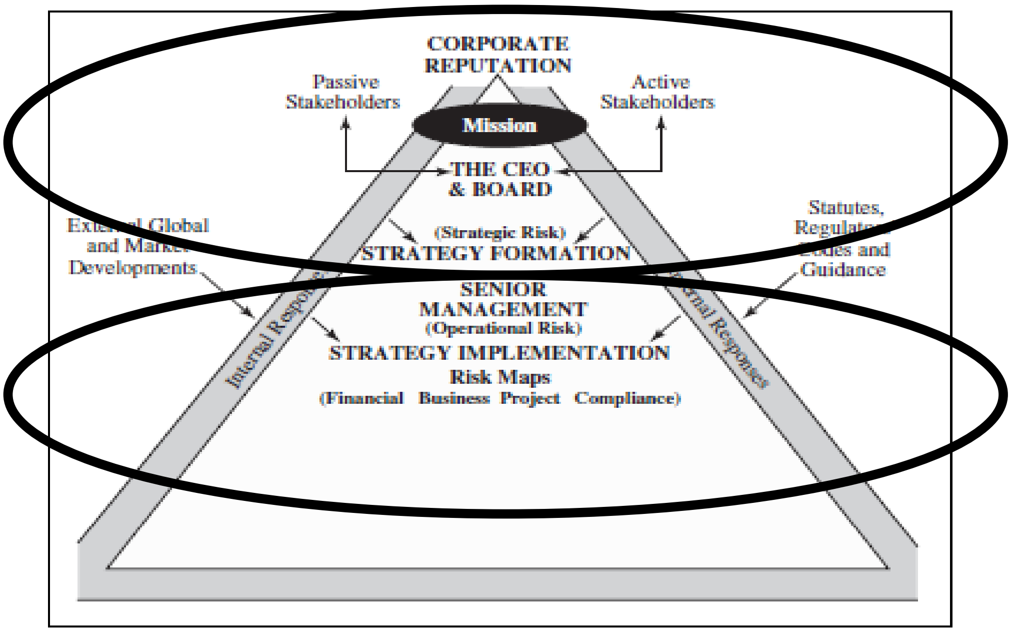


Figure 2.6: Risk management framework model

Source: Spencer Pickett (2005a:10)

The types of risks relating to an organisation as mentioned above are further categorised as:

- Inherent risk; and
- Residual risk.

2.6.3 Inherent risk

Fraser and Simkins (2010:108) are of the opinion that the amount of risk prior to it being treated is called inherent risk, therefore, before mitigation or control is implemented.

Inherent risk is the gross risk faced by an establishment, therefore prior to the organisation implementing an appropriate mitigation or control to deal with such a risk (Pickett, 2005b:62)

Another view relating to the term inherent risk, according to Valsamakis *et al.* (2010:43), refers to all those activities and events that impact on organisational profits.

2.6.4 Residual risk

Residual risk is the available exposure subsequent to the implementation of a mitigation or control, therefore, the untreated portion of the risk remaining (Dubihlela & Nqala, 2017)

Residual risk is also known as the amount of remaining risk subsequent to the application of the appropriate mitigation or controls within the organisation (Fraser & Simkins, 2010:183)

The difference in the inherent risk and residual risk exposure to an organisation is shown below in Figure 2.7.

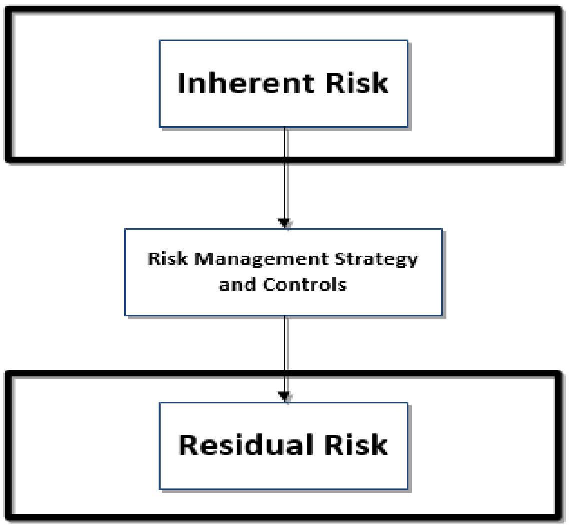


Figure 2.7: Inherent risk and Residual risk

Source: Spencer Pickett, 2005b:61)

2.7 Defining risk appetite

Steinberg *et al.* (2004:28) describe risk appetite as the amount of exposure that an entity will accept to achieve its goals.

According to Fraser and Simkins (2010:287), risk appetite speaks of the extent of the amount of risk the entity will take in the chase of set goals. Another view by Wu, Olson and Birge (2011:283) is that the risk appetite set requires to be communicated throughout the organisation as well as being consistently applied across the entity.

Therefore, organisational staff is required to understand the risk appetite of the entity to differentiate between a worthy and unworthy risk to accept to achieve its goals.

How an organisation perceives residual risk exposure subsequent to applying a suitable strategy is another way of explaining the term "risk appetite". Such exposure could be accepted or not, as illustrated below in Figure 2.8 (Siwangaza & Dubihlela, 2017).

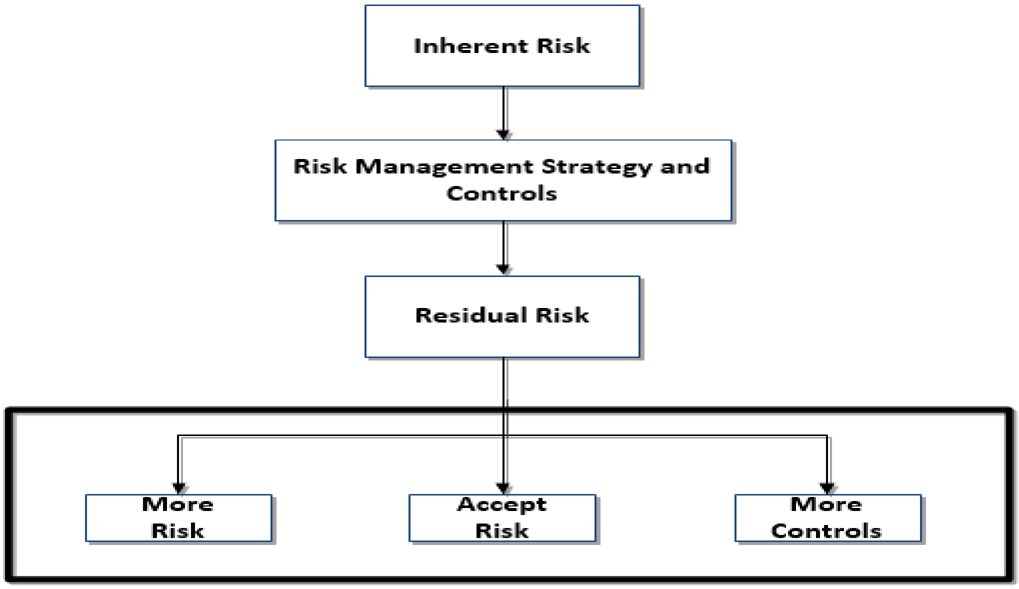


Figure 2.8: Risk appetite

Source: Spencer Pickett (2005b:61)

The responsibility of the board (directors) is to determine the appetite (risk), whilst management is responsible to abide by and implement such information as communicated (Spencer Pickett, 2005a:97).

2.8 Theoretical framework

According to Collis and Hussey (2014:104), the term “theoretical framework” refers to the gathering of theories from applicable literature and supporting a study. It also is an important part of the process, underpinning the research questions.

The term “theory” is further explained by Collis and Hussey (2014:104) as the clarification of how things work and why events transpire. Saunders, Lewis and Thornhill (2016:47) acknowledge that a theory comprises the following elements:

- **What –** Variables are being examined by the theory;
- **How –** Are the variables related;
- **Why –** Are the variables related;
- **Who –** Does the theory apply to;
- **Where –** Does the theory apply; and
- **When –** Does the theory apply.

Adedolapo (2016) includes the use of the Perceived EReadiness Model (PERM) and Structuration theories to uncover and understand implementation factors associated with the BYOD strategy. Bais (2016) includes a theoretical framework focussing on the 11 functional areas of enterprise cybersecurity linked with the use of a BYOD strategy, to understand the associated security issues. Sahd (2015) includes the identification of mobile solution risks and related internal controls as a theoretical basis to understand if the use of matrixes could improve control systems associated with related risks identified.

In Creswell’s (2008:Ch. 3) opinion, when a researcher applies a quantitative research approach to a study, the following theoretical perspectives could be considered:

- Psychology literature;
- Sociological literature; and
- Social psychology literature.

Since the analysis of variables in this study focuses on individuals, psychology literature could be considered, according to Creswell (2008:Ch 3). An observation by Cherry (2019) further clarifies that the behavioural psychology linked to the first theoretical perspective (psychology literature) mentioned above, refers to the learning of behaviours through the different types of conditions an individual has encountered in their lives.

The researcher considers the theoretical framework important for this study. Whilst Adedolapo (2016), Bais (2016) and Sahd (2015) focused more on the implementation factors, security issues and improving of control systems when using a BYOD mobile device strategy in their respective studies, this research focused on the factors associated with the human elements and internal control processes associated with the management of risks linked to the use of mobile devices. Therefore, the behavioural psychology theory, as explained above, was selected and applied in this research. The application of this theory within the study indicates that the introduction and/or permitting of mobile devices for use in the workplace by employees could impact their behaviour and therefore influence productivity and the effectiveness of organisational risk management practices. The application of this theory, further provide structure to the research. As this theory is applied to the study, the researcher would expect that the introduction and/or permitting of mobile device use by organisations to their employees in the workplace (independent variable) to influence the risk management practices within the organisation (dependent variable) as well as the associated employee's productivity (dependent variable).

The applied theory comprises the following:

- **What:** Permitting and/or introduction of mobile device use by employees (within an organisation), risk management practices (within an organisation) and employee productivity (within an organisation) are the variables being evaluated;
- **How:** Does this device use impact/influence an employee's productivity and have an effect on risk management;
- **Why**: An increase in the investment of mitigation in such an instance could lead to more effective risk management, which may positively affect productivity;
- **Who:** Theoretical conclusions might apply to administrative employees utilising mobile devices, but not to operational employees who does not making use of such devices;
- **Where:** Theoretical conclusions might apply at the Namakwa District in the Northern Cape, but not at other districts and/or provinces; and
- **When:** A substantial increase in the investments of mitigation could positively impact the effectiveness of risk management and possibly have an effect on Productivity and therefore requiring a re-evaluation of such theoretical conclusions in future.

Rewards associated with the performance of this study, include:

- Observations noted will inform management whether risk management practices are effective; and

- Findings will also inform management whether employees deem the use of mobile devices as important in achieving organisational objectives.

Further analysis was performed and is detailed in Section 2.11 (empirical study) of this report, which supports the focus of this study.

2.9 Research focus area

The focus area of the study is local government entities within the Namakwa District. Details relating to the population of this study are contained in Section 3.3.2.

2.10 Clarification of entities (municipalities) and research objectives in scope

i) Entities

According to an online overview of the research, the Namakwa District consists of seven municipalities. This includes one District Municipality and six Local Municipalities. The demarcated areas relating to the local government entities within the Namakwa District are shown in Figure 2.9 below.

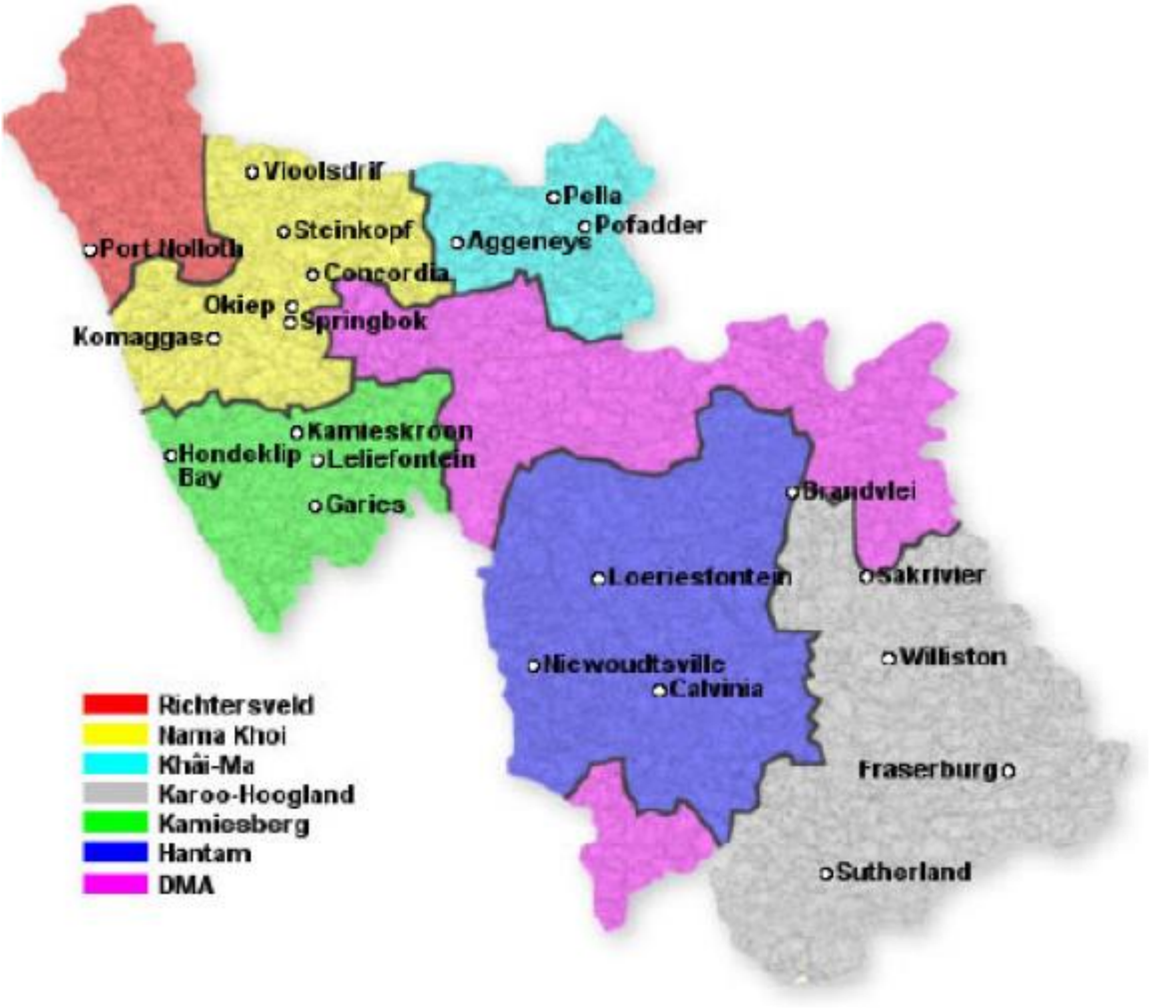


Figure 2.9: Municipalities in the Namakwa District

Source: Bourne, Donatti, Holness and Midgley (2012)

ii) Research objectives

Whist the trend in work habits shifted as employees were able to work from outside the office, according to Wood (2017), security should be well thought through when dealing with risks of uncontrolled devices on an enterprise’s network(s) (Cardinal, 2016). This is supported by past research that confirms that mobile device use currently tops the security risk list. However, Souppaya and Scarfone (2013) opine that security objectives can be achieved through the securing of mobile devices against associated threats. As illustrated above, the shift in working habits to include mobile devices within organisations is a current trend.

The aims of the study are:

i) To understand the importance of mobility to management and employees of local government entities in the Namakwa District in achievement of organisational objectives; and

ii) To understand the effectiveness of risk management where mobile device connections to local government networks are permitted in the Namakwa District.

2.11 Empirical study

Whilst reviewing earlier research, the following was noted.

Brand (2013) confirmed that the implementation of developed best practices and the application of due care whilst utilising mobile devices results in an effective, efficient and optimised cost answer. This could be applied in the mitigation of risks pertaining to the security of enterprise mobility. However, one of the opportunities for further studies confirmed by the researcher relates to the security risks emanating from the operational level whilst utilising mobile devices.

Sahd (2015), in addressing risks associated with mobile devices, identified incorporated controls on three levels (mobile solution governance, management systems and organisational control techniques). However, the researcher noted further research opportunities in unidentified associated risks, as well as the improvement of internal controls (use of matrixes).

Bais (2016) established that risks associated with a BYOD mobile device strategy can be mitigated by mobile device management (MDM) technology and that an effective policy would be a solution as well. Opportunities for further research confirmed by the researcher include the worthiness and cost implications of such a strategy for organisations.

Zimeng (2015) argued that an encryption technique between the mobile device and Virtual Private Network (VPN) prevents information theft by unwanted individuals. However, according to the researcher, opportunities for further research include the verification of other security solutions.

Phillips (2014) confirmed that all aspects relating to the governance of information security are pivotal. It was further noted that organisational governance on its own is not enough to protect an entity's information. Another observation by the study established that there is an important connection between risk management, compliance and information security governance in the process of strengthening the organisational control environment. Opportunities for further studies suggested by the researcher include associated privacy risks as well as organisational information risks.

Lydon (2014) further that entities must exercise care in instances where a BYOD strategy is utilised within their organisations. The researcher notes that an opportunity for further studies relates to the management of compliance risks emanating from the utilisation of mobile devices.

According to Adedolapo (2016), entities should be organisationally and environmentally ready when considering the utilisation of a BYOD strategy. The researcher notes that a further research opportunity exists with regard the mitigation of privacy risks associated with the utilisation of a mobile device strategy (BYOD) using policies.

A study performed by Heijblom (2015) established that an opportunity exists for further research on mobile devices in the development of a methodology relating to risk assessment to prioritise the treatment of higher risk exposure before spending time on the remaining risks.

According to Brodin (2016), opportunities for further research include the performance of awareness training relating to information security as well as the effective communication of related policies within the organisation.

De Shield (2017) confirmed that further opportunities for research include risks pertaining to privacy, compliance and governance.

As confirmed by the review of literature discussed above, the use of mobile devices as an organisational strategy, as well as the type of strategy elected, comes with potential associated risks to the organisation. Further research opportunities suggested in the reviewed literature confirm that the management of risks emanating from the operational level is an area that warrants additional investigation.

Ames *et al.* (2016) confirms the risks relating to the use of mobile devices include exposure such as:

- User privacy risks;
- Physical security risks;
- Organisation and user information security risks; and
- Compliance risks.

It is important to understand that the use of mobile devices could have further associated risks. However, this study was confined to the risks of user privacy, physical security, organisational and user information security and compliance, which are further discussed in section 2.12 below.

2.12 Mobile devices – related risks

2.12.1 User privacy risks

Mobile devices utilised in the past within organisations were mostly laptops, which were supplied by the organisation. However, in recent years this has changed to include strategies such as a BYOD strategy where personnel could utilise privately owned devices for work-related activities. Such an arrangement, however, increases concerns relating to the individual's privacy and the privacy of an entity about its information (Miller, Voas & Hurlburt, 2012; Ames *et al.*, 2016). Dhingra (2016) agrees, indicating that an important factor to consider when implementing a BYOD strategy is an employee's privacy as well as the organisation's rights in terms of monitoring of activities. In cases where an investigation is required for whatever reason, the personal device is retained and therefore results in an employee's personal information on the device being captured.

Privacy of the employee's data that are accessible by the employer should be maintained. However, the employer's sensitive information should also be safeguarded. Since the employee's private information is known to the employer in such instances, it could result in it being used against an employee (Afreen, 2014). This noted by Loose *et al.* (2013) who reasoned that the loss of, as well as retrieval of personal information by organisations, were considered a threat in the use of employee-owned devices.

One of the major challenges relating to the successful roll out of the utilisation of privately owned mobile devices is its monitoring and control without violating the user's privacy. Such a violation could result in users not supporting the initiative, based on the lack of a secure feeling (Hanlin, Jiao, Thomas & Xiaowei, 2013). Therefore, great care must be taken in instances where private and personal information stored on such devices is accessed as it could result in claims against the organisation as well as possible embarrassment to such a user (Hinkes, 2014). An organisational requirement to safeguard important data by implementing controls to ensure that such information not ending up in the hands of competitors or criminals, could be contradictory to the privacy of employees (Hetting, 2014).

Employees travel around with their laptops, tablets and smartphones on a daily basis, not always paying attention or being aware of the possible security and privacy exposure to their business, as well as their personal information. A lack of awareness could result in harm when such information is compromised due to for example loss of such devices and therefore could outweigh the benefits associated with the utilisation of these devices (Garba, Armarego & Murray, 2015).

Where an information breach occurs it becomes problematic for the organisation as personally owned devices are not fully controlled by the organisation, making it challenging to access. The concern for the device owner is that no access will be granted to the device during the investigation and personal information might be retrieved from the device, which could affect user privacy (Dhingra, 2016). Privacy and safeguarding of information could be driven by the organisation in the form of policies and procedures (explained in Section 2.13). These documents could include rules such as the frequency of security updates on devices and not sharing confidential information, to name a few. However, it should also be explained to the user through training and awareness (described in Section 2.13) that if such rules are not being complied with, it could expose the organisation and/or the individual's information. Another consideration is the protection of the physical asset, as explained below.

2.12.2 Physical security risks

Smart devices connected to organisational networks are mobile in nature and utilised in different locations. Therefore, such devices are at risk of being stolen or lost, and could put sensitive organisational information at risk (Ames *et al.*, 2016). Souppaya and Scarfone (2013) support this, indicating that mobile devices are generally utilised at many different locations, not necessary always in the control of the organisation. This increases the likelihood of the device being stolen or lost.

This is confirmed by van Kessel *et al*. (2013), that a growing trend was noticed in the access of information on smart mobile devices being stolen or lost, which indicates that it is of utmost importance that mitigation is developed and implemented to minimise the potential damage in such cases of devices being lost or stolen.

According to Khan, Abbas and Al-Muhtadi (2015), the physical security of mobile devices is seemingly impossible where the user is making constant use of it. Devices being lost and having minimal access safeguards such as password controls could pose a potential risk to organisations (Evans, 2013). This is confirmed by Bellamy

(2014), who reports that almost 50% of the entities in their survey had lost a mobile device. Therefore, physical securing of smart devices connected to organisational networks should be considered as very important (Disterer & Kleiner, 2013).

Physical security risks of mobile devices should be communicated to employees and organisations should consider, amongst others, to furnish such users with a policy or procedure document as explained in Section 2.13, guiding in the process to be followed in cases of devices being stolen or lost.

However, effectiveness of the mitigation might be affected if the owner of the device (the user) does not notify the organisation immediately if the device is lost or stolen (van Kessel *et al.*, 2013). Therefore, further mitigation as explained in Section 2.13, should be considered to create awareness in users about the possible implications for themselves in terms of the user's privacy as discussed in Section 2.12.1, as well as the associated organisation and user information security risks as discussed below in Section 2.12.3.

2.12.3 Organisation and user information security risks

Information stored on mobile devices should be safeguarded and considered just as important as the actual physical device itself. According to Ames *et al.* (2016), data stored on these devices are at risk of being compromised where suitable security is not in place. Another concern is instances where security of such devices is reduced by users, opening the door for potential attacks (Gomez, 2013).

Mobile devices are also utilised to make use of networks outside the organisation for activities such as Internet access. Since the organisation usually does not have control over the security of such networks, information being communicated could be compromised (Souppaya & Scarfone, 2013). Where users use VPN connections, information could be compromised in instances where such devices are lost or stolen and such channels are used by other people (van Kessel *et al.*, 2013).

According to Dhingra (2016), the practice of the BYOD strategy within a business poses many risks but the risk of data being lost is considered one of the biggest threats. Pereira *et al.* (2017) agree that BYOD within businesses in recent times has increased security risks. Keeping of organisational information on a mobile device poses the risk of it being compromised due to the loss of such a device (Hemdi & Deters, 2016). It was further noted that security-related issues are high on the list when considering the use of personal mobile devices, as employees take sensitive information away from the organisation, thereby opening the door for unauthorised utilisation or alteration (Jamaluddin *et al.*, 2015). This was confirmed by Pillay *et al*. (2013), Miller *et al.* (2012), and Hetting (2014), who are of the opinion that such a strategy poses the risk of information loss in the event of a device being lost.

Another concern raised regarding this strategy by Pillay *et al.* (2013) is that in the event of employees making a device change, critical information might land in the hands of unauthorised individuals. This sentiment is supported by Siddiqui (2014), indicating that sensitive information might get lost or compromised where employees dispose of their devices, give them to family or in the event of them exiting the organisation. Business information being lost may result in unfavourable publicity, which could negatively affect stakeholder's confidence in the organisation's systems and controls, as well as its ability to manage its affairs (Hinkes, 2014). Therefore, the benefits associated with this strategy could be outweighed when the organisation's information is not effectively managed (Garba *et al.*, 2015).

If the organisation requires an updated mobile device or if the employee wants to upgrade their mobile device, organisational information should be removed to remove the possibility of such information landing in the hands of unwanted individuals, which could cause harm to the organisation (Dhingra, 2016). According to McDonnell, Fox, Moroney and Wills (2014), updating of the device model and operating system is pivotal, as the likelihood of information being compromised is greater with an older device. It is therefore important to enforce a standard in the form of a policy or procedure as to how the organisation will deal with instances where an employee wants to dispose of the device, loses it or leaves the organisation, to safeguard the entity's information stored on such devices (Hinkes, 2014). According to Sheldon (2013a), the Information Technology department would have to implement processes and controls to improve the management and security of organisational information in the event of such a strategy being implemented.

The balancing of the user's private information, organisational information and protection of the physical asset whilst utilising mobile devices is very important, as discussed in Sections 2.12.1 to 2.12.3; however, compliance with applicable laws and regulations is also crucial, as further explained in Section 2.12.4 below.

2.12.4 Compliance risks

As an organisation, the entity is obliged to comply with certain regulations, laws, policies and procedures to improve stakeholder confidence and continue their operations, resulting in the increase of investors' value. Therefore, in a strategy to utilise smart devices, irrespective whether it is BYOD, COPED or CYOD, an organisation is required to implement the required mitigation to minimise the realisation of such compliance risks.

Whilst utilising smart devices owned by users, organisations rely on users to comply with applicable laws, regulations, policies and procedures (Ames *et al.*, 2016). Another compliance risk would be to maintain the safety of the user's private information such as contacts and photos against organisational access (Disterer & Kleiner, 2013). Employees are often not keen to implement recommended security policies and procedures, and thereby could be expose the organisation (Dhingra, 2016).

Controls should be implemented to drive the compliance of the organisation in terms of the applicable requirements. However, such controls enforced by an entity is another aspect an organisation should guard against, ensuring that it is not in contradiction of laws and regulations (Garba *et al.*, 2015). Therefore, mitigation relating to the use of mobile devices is key, as further explained in Section 2.13 below.

2.13 Mobile devices – related mitigation

The impact of risks pertaining to the use of mobile devices could be reduced when implementing the correct mitigation (Ames *et al.,* 2016). Another opinion of Sahd and Rudman (2016) is that when mobile devices are utilised, adequate and applicable mitigation is pivotal at management, governance as well as operational levels.

Mitigation could be classified as being a preventative, detective or corrective control as explained below (Spencer Pickett, 2005b:98).

- **Preventative** – Controls ensuring that the system is operating as intended in the first place.
- **Detective** – Controls ensuring that the system is detecting errors or omissions within the process.
- **Corrective** – Controls ensuring that the system is correcting errors or omissions found within the process.

The focus of the study was on the mitigation of risks relevant to the use of mobile devices on an operational level as per sections 2.12.1 to 2.12.4 and shown in Figure 2.10 below.

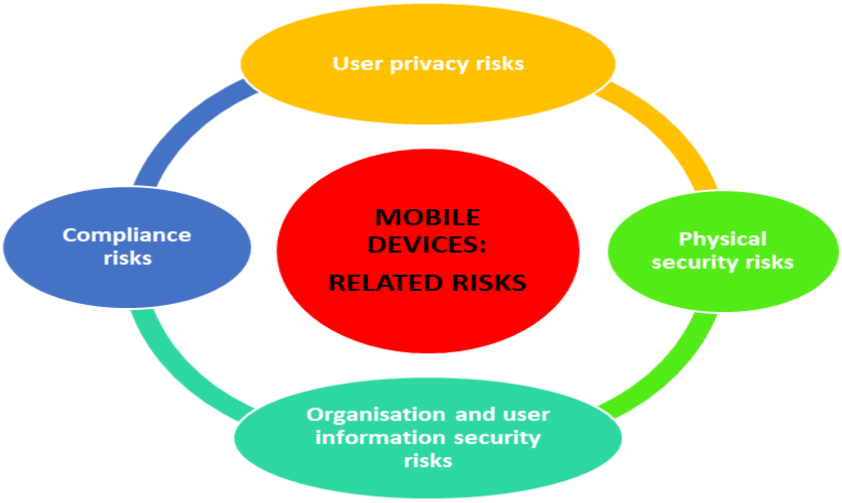

User privacy risks
Compliance risks
MOBILE DEVICES: RELATED RISKS
Physical security risks
Organisation and user information security risks

Figure 2.10: Risks pertaining to the use of mobile devices

Source: Ames *et al.* (2016)

At an operational level, the following mitigation should be considered in the process of risk management (reducing the residual risk exposure) where mobile devices are utilised by an organisation. This is the focus of this study and is further discussed in sections 2.13.1 to 2.13.5.

- Supporting a specific technological solution;
- Managing access requests;
- Developing a security policy and/or procedure;
- Providing user training and awareness sessions; and
- Monitoring and maintenance of records relating to users having such access.

2.13.1 Technological solution supported

The decision around the supporting of a specific technological solution for the organisation is very important, assisting in the securing of organisational information. However, this could vary from organisation to organisation, as it is a risk-based decision.

According to Souppaya and Scarfone (2013), organisations strive to limit access to their network and will therefore support a specific strategy (BYOD, COPED or CYOD). A solution supported by the entity might also include the limiting of the type of access for one strategy (BYOD), whilst giving access in the case of another (COPED), dependent on the most and least control the organisation has over a specific device.

Rowton (n.d.) argues that the implementation of a strategy to minimise the types of devices allowed to access the entity's network could be beneficial because it reduces the knowledge required by Information Technology personnel relating to different types of devices.

Irrespective of the type of strategy an entity supports, controls relating to the safeguarding of information should be a key element. A form of such a control is explained by Disterer and Kleiner (2013), in that organisations should be able to remotely clean out data from a lost device or in instances where users' employment is terminated. All such information should be included in the entity's policy and/or procedure documents. However, another important factor to be included in such a document could be management of access requests as discussed in Section 2.13.2 below.

2.13.2 Management of access requests

Organisations should consider performing a risk assessment, taking into consideration factors such as employees' job functions, conditions or environment of work and years of service with the organisation to ascertain the inherent risk exposure to the business and whether the organisation is willing to accept the risk or if it should consider implementing mitigation prior to permitting access to their network(s) with smart devices. This is supported by Vignesh and Asha (2015), stating that access with mobile devices to corporate networks should be restricted and only provided to employees based on grade and job description, whilst Souppaya and Scarfone (2013) are of the opinion that the type of mobile devices allowed to access organisational resources should be defined. This approach is confirmed by Revenaugh and Schweigert (2013), indicating that organisations initially only provided access with mobile devices to organisational data, to a selected group within the executive management.

According to Rowton (n.d.), admissibility criteria relating to which employees qualify for access with such devices and which employees do not qualify, as well as the required approvals should be included within the entity's policy and/or procedure document/s developed, as further explained in Section 2.13.3 below.

2.13.3 Development of security policies and procedures

It is advisable for organisations to develop and implement a privacy and security policy, providing guidance to employees, as well as to protect organisational information (Garba *et al.,* 2015). A privacy and security policy is a set of rules, known throughout the organisation, which should be followed by employees (Lima, Sousa, Cruz & Simoes, n.d.). According to Yevseyeva *et al*. (2014), this policy should be considered as a measure to be complied with, in protection against security risks. It should also be noted that an inflexible privacy and security policy might trigger employee rebellion, which could ultimately result in circumventing it. This was further confirmed by Larson and Weil (2013), indicating that the use of smart phones for business purposes brings related policies into focus. However, Miller *et al.* (2012) are of the opinion that the likelihood of security policies and/or procedures being enforced is smaller in instances where organisations do not own such devices.

This is confirmed by Souppaya and Scarfone (2013), stating that the improvement of security of mobile devices requires the implementation of policies and procedures relating to the selected strategy being implemented. In the event of the utilisation of a BYOD strategy for example, users are impacted directly by security-related issues. It is advisable to include these users in the crafting of such privacy and security policies (Hanlin *et al.,* 2013). Bellamy (2014) reports that entities require strong policies in the event of such a strategy to minimise the possibility of an information breach.

Therefore, the items considered for inclusion within the BYOD policy, based on the opinion of Dhingra (2016), should be:

- Securing of mobile devices;
- Encryption and passwords;
- Categorisation of information or data;
- Installation of anti-virus software;
- Accessing information wirelessly;
- Remote access (working), and
- Privacy preservation.

Further to the abovementioned considerations, Hinkes (2014) states that the listed items below should also be considered for inclusion in the list:

- Preservation of employer secrecy (trade secrets and data),
- Cost and ownership issues;
- Working together in terms of policies;
- Agreement and buy-in from employees; and
- Training of employees.

However, during the development of these specific policies and procedures, the originator should also consider the rollout, training and awareness associated with these documents to ensure alignment of the users, as further explained in Section 2.13.4 below.

2.13.4 User training and awareness

The development and implementation of a new policy and/or procedure document should be rolled out in an appropriate way to ensure that the awareness of the process is communicated to the relevant audience as well as the necessary training provided.

According to Harris *et al.* (2013), awareness is only the first level within the process and should not be considered as training. Their opinion is that training takes considerably longer and would require active involvement, resulting in the development of the user. This is confirmed by Disterer and Kleiner (2013) as well as Siddiqui (2014), indicating that a comprehensive training exercise is essential for users when implementing a new policy or procedure document.

Hanlin *et al.* (2013) record that through training and awareness sessions, users would become more vigilant about security whilst utilising these devices. Another consideration that is as important as the management of access requests, development of the required policies and procedures as well as the training of users, is the monitoring element of the maintenance and monitoring of user records, as discussed in Section 2.13.5 below.

2.13.5 Maintenance and monitoring of user records

Record keeping of assets in the form of an asset register is a control that has been in place for decades and should be a consideration in this new era where mobile devices have access to organisational networks.

According to Souppaya and Scarfone (2013), keeping an inventory list of all mobile devices having access to the network, including data such as type of access, and user information, would be a good practice. In performing such an exercise, other mitigation such as subsequent assessments could be performed to ascertain whether the user still needs the access initially granted or taking away access of user, considered to be more risky now than the when the original assessment was conducted.

Therefore, risk management is key and requires effort from all individuals from top to bottom within the organisation, as discussed in Section 2.14 below.

2.14 Risk management – roles and responsibilities

The strategy to utilise mobile devices within the organisation presents risks or exposure to the business, as earlier clarified. As previously mentioned, these risks should be managed as part of a process, ensuring that the residual risk exposure is within the entity's limits and therefore acceptable to the organisation. Risk management within the entity should be considered as important throughout the entire organisation and driven by all in the organisation.

The roles and responsibilities of the different levels of risk management are explained below.

2.14.1 Roles and responsibilities - Executive Authority (Municipal Council)

According to Section 21 of the South African Local Government Association (SALGA) Risk Management Framework:

> The Executive Authority should take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the Institution against significant risks.

It is further noted within Section 21(2) and Section 21(3) of the SALGA Risk Management Framework that the Executive Authority's responsibility pertaining to the management of risks, includes:

- Organisational strategies and government's mandate is aligned;
- Ensuring that the organisation's strategic decisions are based on robust risk assessments;
- Key inherent risks associated with the organisation's strategies are identified, assessed and governed;
- Supporting the Accounting Officer dealing with risks beyond their control;
- Ensuring the achievement of objectives, effective performance management;
- Approving the policy pertaining to risk management; and
- Approving of the strategy (SALGA, n.d.)

2.14.2 Roles and responsibilities of the accounting officer (management)

As previously noted, the Executive Authority (Municipal Council) of an organisation is responsible for decisions on the risk strategy and risk management policy. In accordance with Section 60 of the Municipal Finance Management Act (MFMA) the municipal manager within a local government entity is the accounting officer of such an entity (South Africa, 2003). According to MFMA Section 62 (1) (c) and Section 95 (c) (i), the accounting officer within a local government organisation is responsible for the management of finance administration and must take appropriate action to ensure that the organisation maintains efficient, effective and transparent systems on the management of risk, finance and internal control. Therefore, the implementation of decisions taken by the executive authority on the management of risk within the organisation is driven by the accounting officer (management).

According to Section 22 of the SALGA Risk Management Framework, the accounting officer is the ultimate chief risk officer of the institution and is accountable for the institution's overall governance of risk.

A summary of activities considered for inclusion in the executive authority and management responsibilities are depicted in Figure 2.12 below. It also illustrates items which the internal audit function should not undertake to perform. The internal audit function's roles/responsibilities are explained in section 2.14.3 below.

2.14.3 Roles and responsibilities of the internal audit function

The purpose of this function, their authority as well as its duties are included in an audit charter document that is formally presented by the Chief Audit Executive (CAE) for approval by the board (directors), in line with Standard 1000, as issued by the Institute of Internal Auditors (IIA) (Kim, Shulman, Hersh & Keister, 2012:18). It was also confirmed by Moeller (2009:542), that the internal audit charter document should be approved by the audit committee (AC). Another responsibility of the AC includes the approval of the internal audit plan (IAP) as well as its budget (Moeller, 2009:543).

According to the MFMA Section 166 (1) all municipalities must have an AC, whilst Section 166 (5) confirms that all AC members must be appointed by the council and that councillors are not allowed to be an AC member. Section 165 (1) of the MFMA further confirms that municipalities must have an internal audit function, whilst Section 165 (2) (a) of the MFMA states that a risk based audit plan must be prepared for each financial year.

In accordance with standard 1210 as published by the IIA, the function should be properly staffed with the correct knowledge and skills mixture collectively within their team to perform the required engagement reviews throughout the organisation, as included in their IAP (Kim *et al*., 2012:27).

Internal audit is defined as an independent function, providing assurance and consulting services with the objective to improve the operations and internal business processes of an entity. The systematic disciplined approach followed during their processes include the evaluation of the adequacy and effectiveness of risk management, governance and control processes (Spencer Pickett, 2005a:3).

As explained above, the internal audit services could be consultative in nature. This type of service includes the providing of advice to management, helping them to improve their internal business processes. The nature and scope of such engagements are normally agreed between this function and management, based on the specific request from management. This function should however guard against stepping over the line in such engagement, as they should maintain their objectivity and not assuming any management responsibilities (Spencer Pickett, 2005a:35). However, where it is known or becomes known by the CAE that the internal audit team does not have the required skills and knowledge relating to the consulting engagement, such reviews should either be rejected or the required skills should be sourced by the function (IIA Standard 1210.C1) (Spencer Pickett, 2005b:136).

The assurance role, on the other hand, includes the providing of assurance services to the AC on the adequacy and effectiveness of processes pertaining to the management of risks, governance and controls within the organisation (Spencer Pickett, 2005a:35). This is further emphasized by Fraser and Simkins (2010:61), stating that the role of the function is to deliver assurance services relating to the risk management processes and therefore they should not undertake to develop or be involved in the development of risk management processes for approval.

The function's roles in the management of risk is illustrated in Figure 2.11 below.

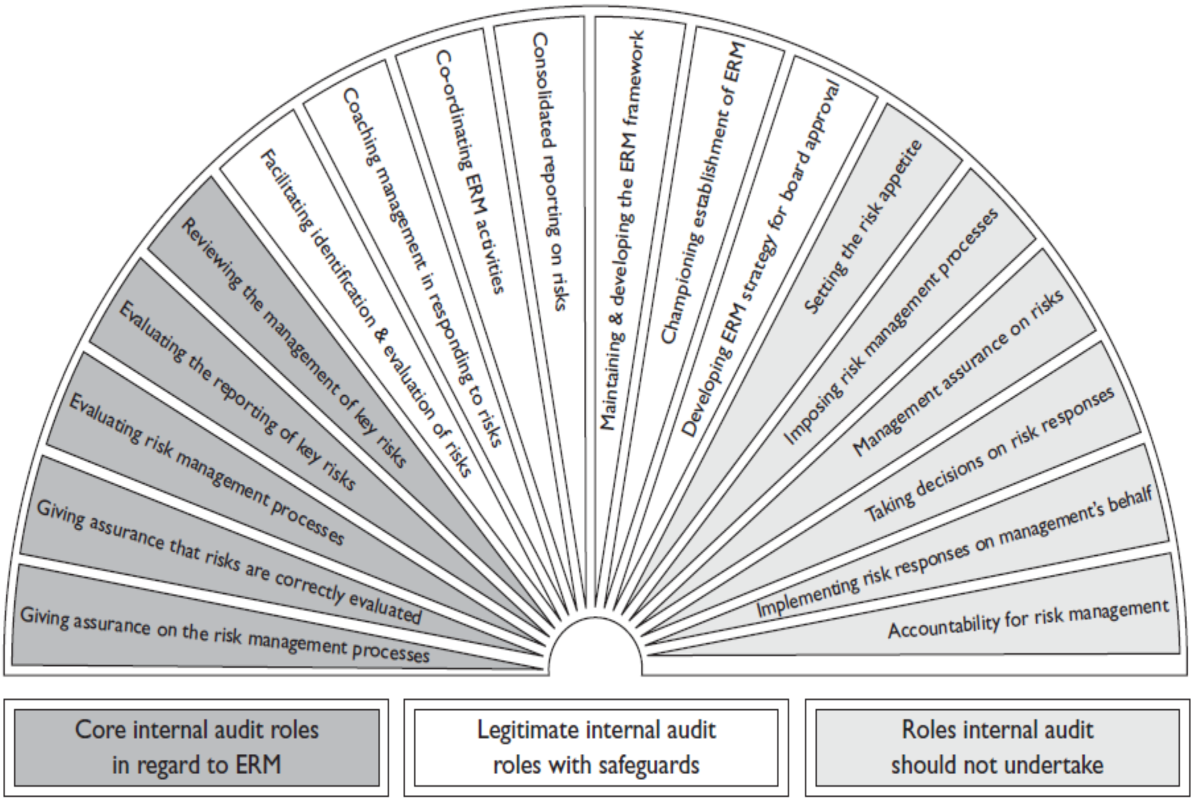

Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing ERM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake

Figure 2.11: Role of Internal Audit in the risk management process

Source: Hopkin (2010:303)

According to Steinberg *et al.* (2004:88), the function is important in the evaluation of the effectiveness of risk management, whilst also providing recommendations relating to its improvement. They are also involved in the reviewing of risk management, governance and control processes whilst assessing and reporting on the below areas:

- Reliability of information;
- Effectiveness and efficiency of operations; and
- Compliance with applicable laws and regulations.

This is confirmed by Spencer Pickett (2005a:111-112), that the key elements to be considered during their review and reported on by the internal audit function, are the three areas as mentioned above, but also include a forth item relating to the safeguarding of an organisation’s assets.

The internal audit function is further required by the IIA standards, more specifically Standard 2440.A1, to communicate engagement results to the relevant stakeholders, where it will be receiving the required consideration and attention (Kim *et al*., 2012:38). Therefore, the internal audit function is obligated to communicate engagement results in the form of an internal audit report to the relevant management team within the scope of the review, as well as communicating results to the audit committee to ensure that the information reported on will be receiving the required attention in line with the IIA standards.

A system to monitor the results communicated to the business in their internal audit reports is required to effect the follow up process. This system will assist in the monitoring process to ensure that actions promised to be taken by the management team are effectively implemented, and where no action is committed to by management on identified weaknesses or gaps within their internal business processes by the internal audit function, that such risks are formally accepted by senior management in compliance with Standard 2500.A1 of the IIA standards (Kim *et al*., 2012:36).

Therefore, in summary, the strategy implemented (use of mobile devices) and the management of related risks is within the role of the executive authority and accounting officer within a local government entity, in line with the risk management process as discussed in Section 2.4 and Section 2.5.

The role of the function in this regard is to review the risk management process to establish the adequacy and effectiveness of the process, as well as the communication of the related results to the relevant platforms and officials, to initiate corrective actions where required.

2.15 Summary: Risk management in the utilisation of mobile devices in the local government entities in the Namakwa District.

The review of available literature on the topic confirms that there are potential risks associated with device use within organisations. Therefore, where entities within local government of the Namakwa District opt to utilise such a strategy, an effective risk management system is important.

The analyses on information on the use of mobile devices in local government entities in the Namakwa District, and the effectiveness of their risk management practices (mitigation) at an operational level, are limited. The analyses are limited to supporting a specific technological solution, management of access requests, development of security policy/procedure, providing user training and awareness and monitoring and maintenance of records associated with users with mobile device access. This is further explored in Chapter Four.

The results pertaining to the analyses performed were used to respond to the study objectives and research questions previously discussed.

2.16 Chapter summary

The utilisation of mobile devices in the business world is a fast growing trend, which requires sufficient time and resources to mitigate associated risks. This chapter defined mobile devices and the risks relating to the use of such devices. It further provided an explanation of the important terms such as risk, risk appetite and risk management utilised, as well as the objectives relating to organisational information. The chapter discussed the elements to be considered in assessing and deciding on the utilisation of mobile devices as well as available options (BYOD, COPED or CYOD) from which to select. Related risks pertaining to the use of such devices were described, as well as possible mitigation, which could be considered at an operational level to reduce the risk exposure associated with the use of such a strategy. Roles relating to the different defence lines within the risk management process were also clarified in this chapter.

The following chapter, Chapter Three, discusses the research design and methodology of this study, which will provide details of the research objectives, research question and sub-questions, population, sampling and the research approach followed.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter addresses the methodology and design of the study and explains the question, sub-questions and objectives. The research focus is on the risk management processes and practices in the use of mobile devices in local government entities in the Namakwa District, Northern Cape. The research employed a structured questionnaire, which included closed-ended questions, providing the participants with a predetermined list of replies from which to select

The layout of this chapter is illustrated in Figure 3.1 below.

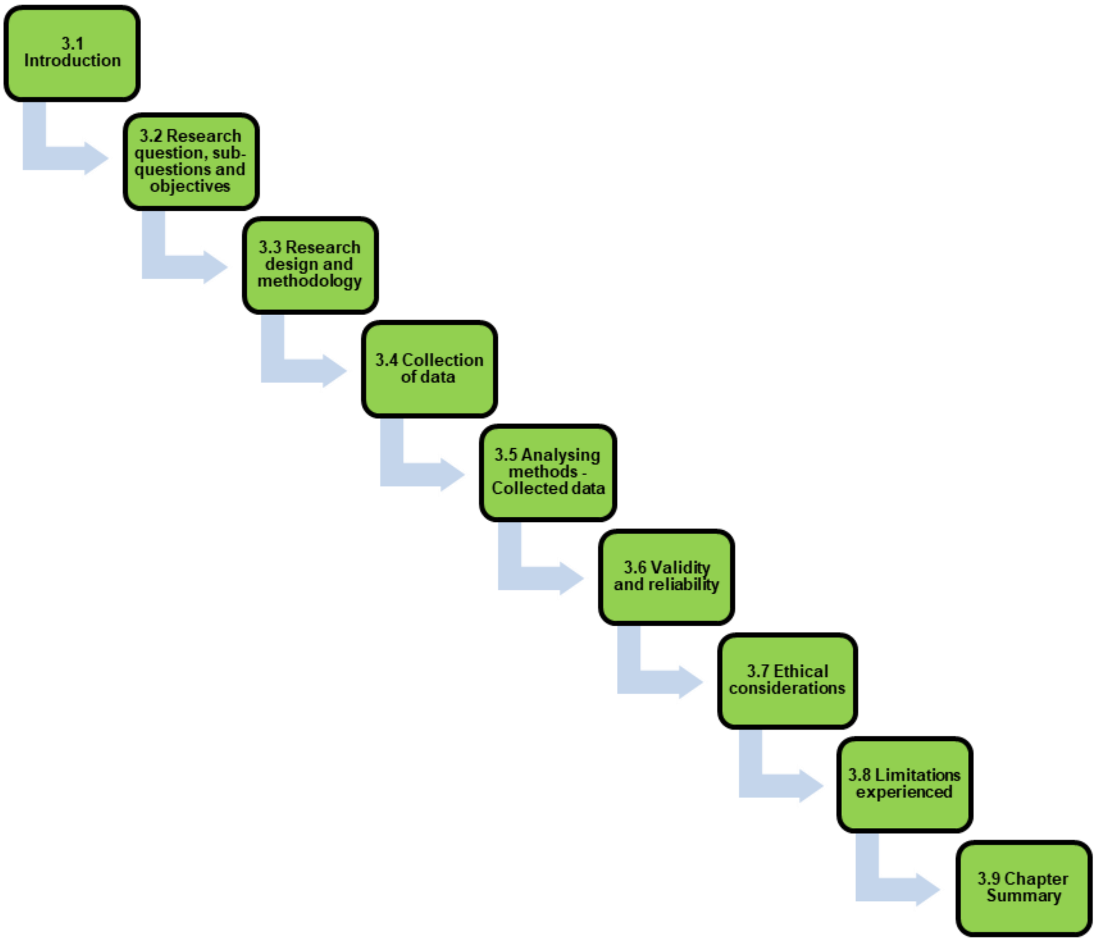

3.1 Introduction
3.2 Research question, sub-questions and objectives
3.3 Research design and methodology
3.4 Collection of data
3.5 Analysing methods - Collected data
3.6 Validity and reliability
3.7 Ethical considerations
3.8 Limitations experienced
3.9 Chapter Summary

Figure 3.1: Layout of Chapter Three

3.2 Research question, sub-questions and objectives

The research question, sub-questions as well as the research objectives relating to this study were explained in section 1.5.

3.3 Research design and methodology

The research design and methodology applied in this study is explained below.

3.3.1 Research method and approach followed

Whilst reviewing available research approaches which could be followed during a study, it was established that research performed could either be quantitative or qualitative (Collis & Hussey 2014:5-6). Beech (2015:33) reports that a qualitative or quantitative research method could be applied.

Explanations and differences between the approaches are addressed below.

i) Qualitative Research

According to Farnsworth (2019), qualitative research produces non-numeric data and includes methods such as individual interviews, which are appropriate for exploratory studies. This is confirmed by Stumpfegger (2017), who states that qualitative research is exploratory in nature and attempts to provide explanations.

ii) Quantitative Research

According to Goertzen (2017), quantitative research produces numeric data and therefore focuses on information that is measurable and permits statistical examination. This was confirmed by Farnsworth (2019), explaining that quantitative research focuses on numbers and figures in an attempt to measure and reveal patterns (behaviour, emotion) in the data.

This research sought the views of employees in local government entities located in the Namakwa District of the Northern Cape. Therefore, it follows a quantitative research approach. This approach was selected as it assists in the measurement and identification of patterns used in responds to the research questions and objectives.

Therefore, the data collection process included the use of a research questionnaire survey that contained closed questions (Sekaran & Bougie 2013:150). This provides the participants in the research process, with a predetermined list of responses from which to select.

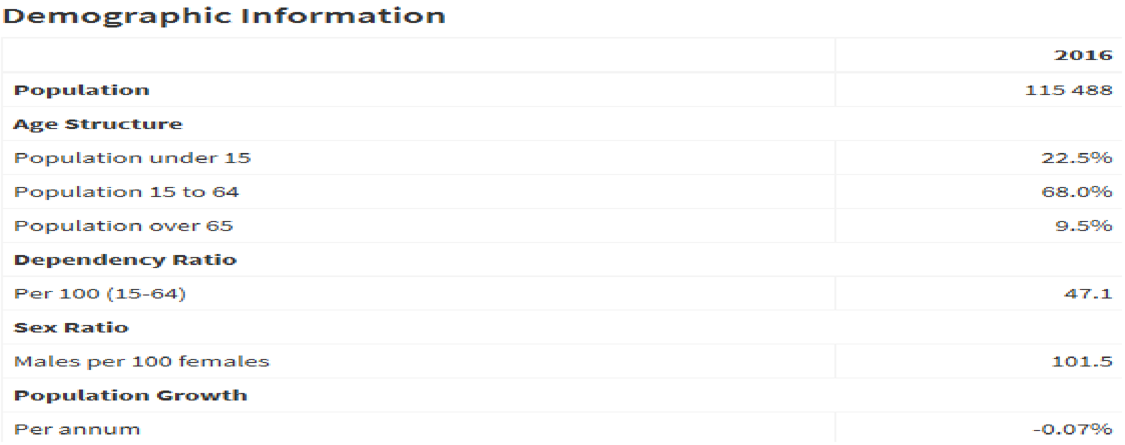
3.3.2 Population

Collis and Hussey (2014:197) describe a population as a specific group of individuals, entities or items considered for statistical purposes. Kenton (2019) is of the opinion that a population is a pool of objects or people from which a sample is selected for statistics. Another explanation of the term “population” by Ragab and Arisha (2017), describe it as a representation of the universe of units from where a sample is selected.

According to an online overview, the research focus area of the Namakwa District equates to 126,836km² and comprises seven entities. This includes one District Municipality and six Local Municipalities (Municipalities of South Africa, 2020:online). Therefore the total number of individuals employed in the administrative functions of these entities (using mobile devices), were considered to be the targeted population for this study.

The seven entities included in the Namakwa District are:

1) Namakwa District Municipality



Demographic Information

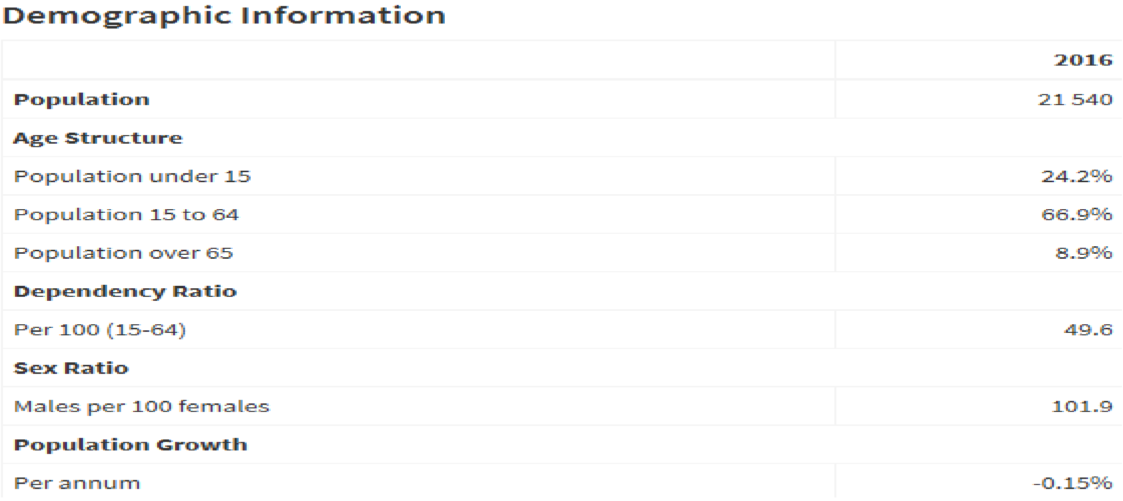
	2016
Population	115 488
Age Structure	
Population under 15	22.5%
Population 15 to 64	68.0%
Population over 65	9.5%
Dependency Ratio	
Per 100 (15-64)	47.1
Sex Ratio	
Males per 100 females	101.5
Population Growth	
Per annum	-0.07%

Employment statistics

Employment	**2016/17**
Number of Positions	125
Positions Vacant	14
Percentage of Vacancies	11.20%

Source: Municipalities of South Africa (2020:online).

2) Hantam Local Municipality



Demographic Information

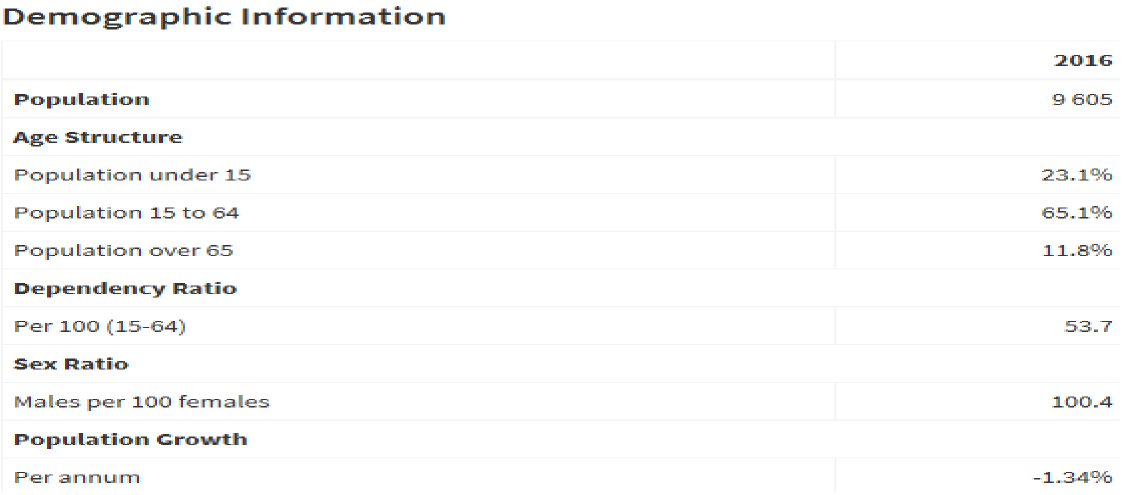
	2016
Population	21 540
Age Structure	
Population under 15	24.2%
Population 15 to 64	66.9%
Population over 65	8.9%
Dependency Ratio	
Per 100 (15-64)	49.6
Sex Ratio	
Males per 100 females	101.9
Population Growth	
Per annum	-0.15%

Employment statistics

Employment	2016/17
Number of Positions	185
Positions Vacant	20
Percentage of Vacancies	10.81%

Source: Municipalities of South Africa (2020:online).

3) Kamiesberg Local Municipality



Demographic Information

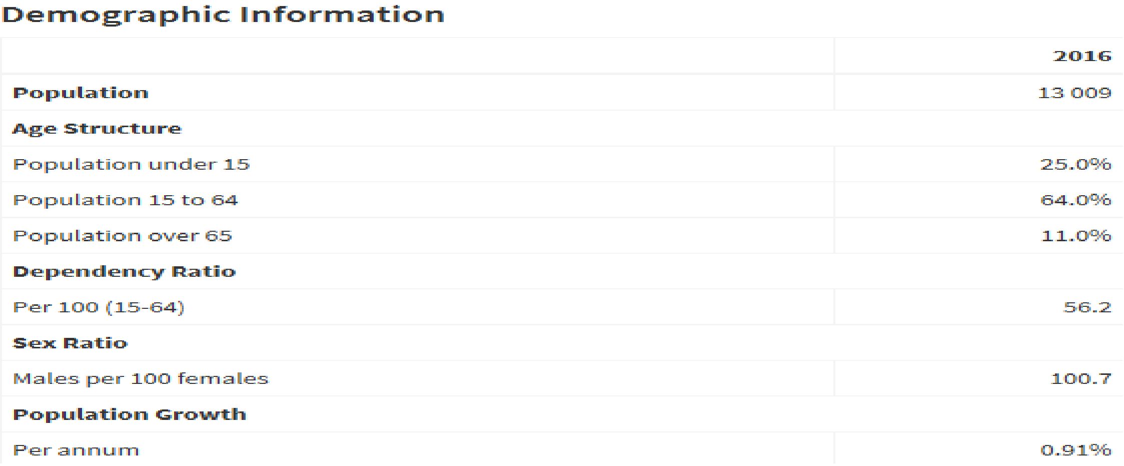
	2016
Population	9 605
Age Structure	
Population under 15	23.1%
Population 15 to 64	65.1%
Population over 65	11.8%
Dependency Ratio	
Per 100 (15-64)	53.7
Sex Ratio	
Males per 100 females	100.4
Population Growth	
Per annum	-1.34%

Employment statistics

Employment	2016/17
Number of Positions	104
Positions Vacant	6
Percentage of Vacancies	5.77%

Source: Municipalities of South Africa (2020:online).

4) Karoohoogland Local Municipality



Demographic Information

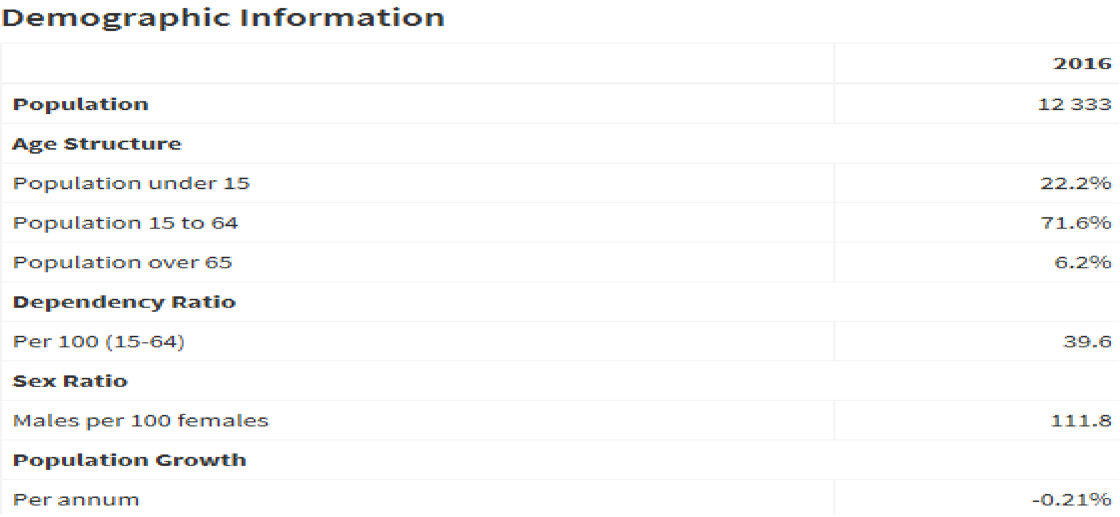
	2016
Population	13 009
Age Structure	
Population under 15	25.0%
Population 15 to 64	64.0%
Population over 65	11.0%
Dependency Ratio	
Per 100 (15-64)	56.2
Sex Ratio	
Males per 100 females	100.7
Population Growth	
Per annum	0.91%

Employment statistics

Employment	**2016/17**
Number of Positions	90
Positions Vacant	26
Percentage of Vacancies	28.89%

Source: Municipalities of South Africa (2020:online).

5) Khai-Ma Local Municipality



Demographic Information

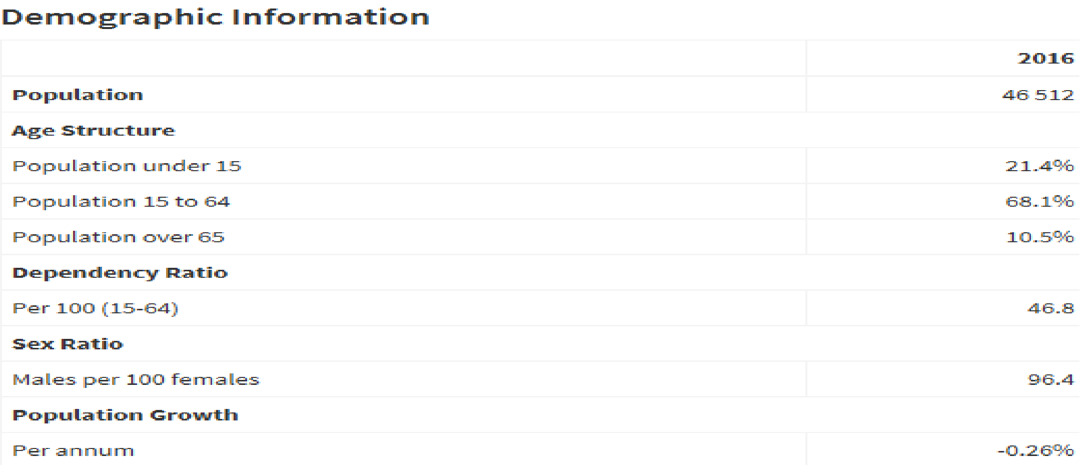
	2016
Population	12 333
Age Structure	
Population under 15	22.2%
Population 15 to 64	71.6%
Population over 65	6.2%
Dependency Ratio	
Per 100 (15-64)	39.6
Sex Ratio	
Males per 100 females	111.8
Population Growth	
Per annum	-0.21%

Employment statistics

Employment	2016/17
Number of Positions	93
Positions Vacant	5
Percentage of Vacancies	5.38%

Source: Municipalities of South Africa (2020:online).

6) Nama Khoi Local Municipality



Demographic Information

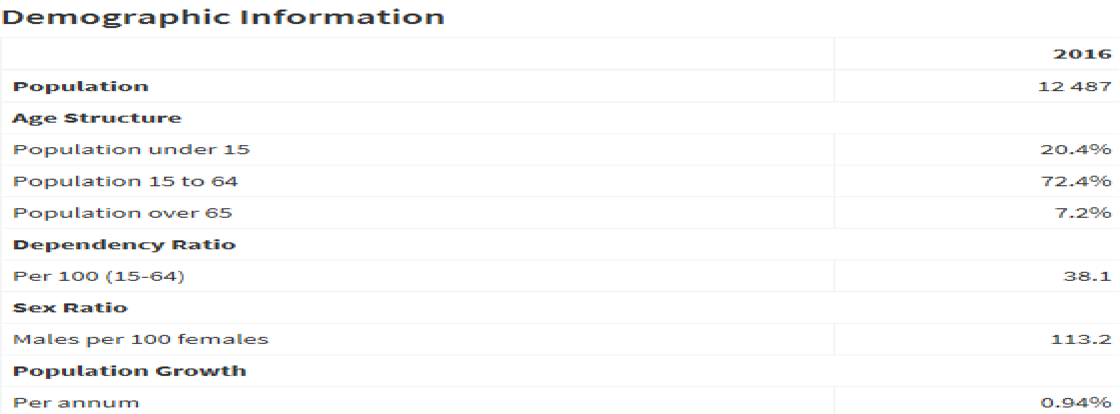
	2016
Population	46 512
Age Structure	
Population under 15	21.4%
Population 15 to 64	68.1%
Population over 65	10.5%
Dependency Ratio	
Per 100 (15-64)	46.8
Sex Ratio	
Males per 100 females	96.4
Population Growth	
Per annum	-0.26%

Employment statistics

Employment	2016/17
Number of Positions	310
Positions Vacant	3
Percentage of Vacancies	0.97%

Source: Municipalities of South Africa (2020:online).

7) Richtersveld Local Municipality



Demographic Information

	2016
Population	12 487
Age Structure	
Population under 15	20.4%
Population 15 to 64	72.4%
Population over 65	7.2%
Dependency Ratio	
Per 100 (15-64)	38.1
Sex Ratio	
Males per 100 females	113.2
Population Growth	
Per annum	0.94%

Employment statistics

Employment	2016/17
Employee Positions	135
Positions Vacant	17
Percentage of Vacancies	12.59%

Source: Municipalities of South Africa (n.d.: online)

3.3.3 Sampling

According to Bhat (2019), the term “sample” refers to, “a smaller set of data that are chosen from a larger population by using a predefined selection method”.

It is acknowledged that the bigger the sample size tested, the better representation provided in terms of the population. However, it is not always possible to select a bigger sample size due to time limitations or constraints during a project. This is confirmed by Beech (2015:84), where he claims that in cases of sample sizes being too small, confidence in the results is lacking. According to Saunders *et al.* (2016:279), the greater the sample size selected, the smaller the possible error relating to the population.

Whilst reviewing the types of sampling approaches that could be followed during a study, it was noted that a sample could be random as well as non-random

(Flick, 2015:101-103). In the opinion of Saunders (2016:276), the non-random (non-probability) selection of a sample can be further broken down into quota, snowball, purposive, self-selection and convenience options as illustrated in Figure 3.2.

The non-random (non-probability) sample selection options were applied during this research and include snowball as well as convenience options. The convenience option involves the haphazard selection of a sample (Saunders *et al.,* 2016:304), whilst the snowball option involves the selection of an initial sample, which further identify others in the population, creating a snowball effect (Saunders *et al.,* 2016:303).

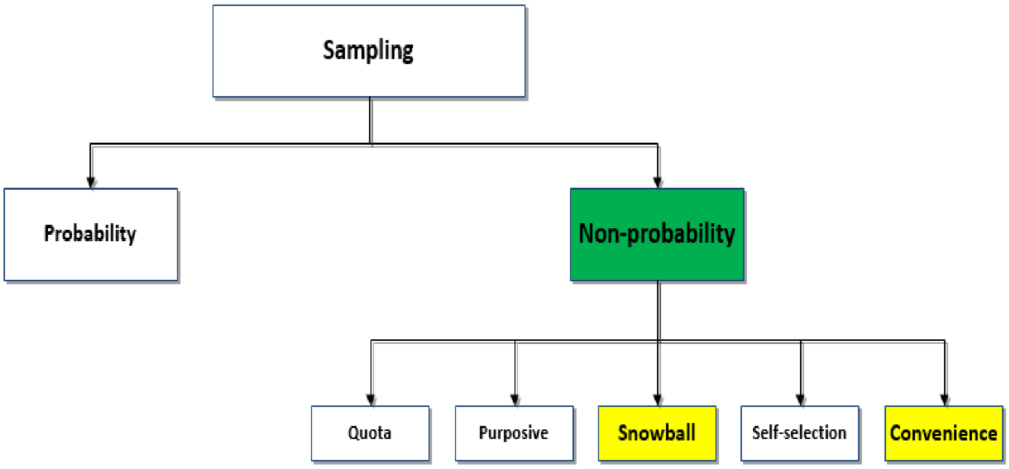


Figure 3.2: Sampling techniques

Source: Saunders *et al.*, 2016:276)

The decision to apply these approaches is because the research focuses on a specific sample of employees in the Namakwa District (administrative function employees making use of mobile devices).

Entities in the Namakwa District were approached to be included in the study as the selected sample organisations. The leadership of five entities formally agreed to partake in the research. The research questionnaires were distributed via e-mail to a contact person in these municipalities. Thereafter, sampling followed the snowball technique as explained above, whereby it was distributed to individuals working in administration functions and who use mobile devices during the performance of their duties.

3.4 Collection of data

This section provides an explanation relating to the data collection method utilised during the study. This includes the research questionnaire design, pilot testing and the process relating to the collection of data.

3.4.1 Data collection method

The information gathering method applied during the study included a research questionnaire distributed to a sample of individuals as described in section 3.3.3 above, to collect data from these respondents for analysis.

According to Remenyi (2013:93), an advantage of the use of a research questionnaire during the research is that it allows for an easier collection of information at a low cost.

Another important consideration to perform is a pilot test prior to the distribution of the questionnaires. This is done to ascertain whether the document contains any areas which require improvement (Remenyi, 2013:122).

3.4.2 Research questionnaire design

The instrument utilised during data collection was a research questionnaire containing seven sections, which are explained below.

Section A – Respondent and enterprise information

This section provides information on the enterprise and respondents. It collects information such as the age category, gender, experience (years) and seniority (position in organisation) of the respondent, as well as the number of employees employed in the enterprise.

Section B – Mobile device connections to enterprise networks: Entity

This section collects information on whether the enterprise make use of mobile device connections on their computer networks, as well as the length of time such connections are allowed and also whether such connections include remote access. It also provides information on which type of devices are mainly utilised, and whether personal mobile devices could also be connected.

Section C – Mobile device connections to enterprise networks: Employees

This section obtains information on the importance of mobile device connections to the entity’s network for employees and the time spent with such devices on these networks. It further also collect data on whether employees agree or not, that the mobile device use enhances their efficiency and productivity.

Section D – Mobile device connections to enterprise networks: Risk management

This section obtains data pertaining to the existence of a risk management function and a risk management system. It further collects data on whether the entity experienced an information security breach since permitting the connection of mobile devices to their network.

Section E – Mobile device connections to enterprise networks: Mitigation

This section obtains information on whether organisations have mitigation in place to manage associated risks (mobile devices).

Section F – Management of risk within the enterprise

This section collects information on whether organisations effectively manage risks pertaining to the use of mobile device connections to the entity's network as well as the management of risk within the organisation in general.

Section G – Contact details of respondent

This section provides the location and contact details of the respondent to provide a trail as well as enable validation of the questionnaire. The research questionnaire (Appendix C) as well as the research participation letter and consent form (Appendix D) are included as appendices.

3.4.3 Pilot testing of research questionnaire

The research questionnaire was pilot tested to ascertain whether any difficulty exists on the completion of the document by the respondents, as well as to establish the average completion time.

The test was performed with four individuals working in the local government sphere, located in the Namakwa District during the month of June 2018. The individuals selected for testing included one senior manager, one middle manager and two individuals from the non-management group. The respondents in this trial test spent 15 minutes on average to complete the research questionnaire, whilst also not experiencing any difficulty in the completion of the document.

3.4.4 Research questionnaire distribution

To obtain information from the selected sample for analyses, the research questionnaires were distributed via e-mail to respondents in line with Section 3.3.3 as discussed above.

3.4.5 Collection of responses

The research questionnaires were distributed via e-mail to the sampled individuals working in the selected municipalities, utilising the sampling approach as previously discussed.

Whilst employing this sampling approach, completed research questionnaires were received by the researcher. Completed documents were sent by the respondents to the e-mail address of the researcher in a PDF format during the period of June 2018 and July 2019. A data analysis was conducted on the responses received, which is discussed in Chapter Four.

3.5 Analysing methods: Collected data

Analysis of information is explained by Prathapan (2014:121) as a process performed by a researcher to convert information to facilitate meaningful interpretation of such data.

Information obtained from the completed research questionnaires was recorded by the researcher in a Microsoft Excel template. This recorded information was provided to the statistician for analysis using the SPSS software.

The following analyses (inferential statistics) were performed and reported by the researcher as per Section 3.6 below:

- Validity analysis;
- Reliability analysis; and
- Correlation analysis.

Descriptive statistics were performed and are discussed in section 4.4.

3.6 Validity and reliability

Validity

Validation of information is of the utmost importance in the research process. It entails the inspection of the data collected for errors and inconsistencies, resulting in more confidence in the information obtained (Callegaro, Manfreda & Vehovar 2015:179).

A research questionnaire was the data collection instrument to obtain information from participants. The questions in the questionnaire were derived from the literature review to ensure alignment to the research questions and research objectives. Questions were designed in a way that could be easily understood by participants. The questionnaire was pilot tested prior to being administered to the rest of the targeted participants, as explained in section 3.4.3.

Furthermore, the researcher performed a correlation analysis to confirm the validity of information obtained.

Reliability

Reliability of information is also important in the research process. This refers to the accuracy of the results in cases of the research being re-performed by another researcher (Collis & Hussey, 2014:217).

The data were collected via a questionnaire which was completed by the participants in their own environments, therefore feeling comfortable and not being pressurised whilst completing the document. The data received from participants were assessed for reliability, using Cronbach's alpha analysis.

Cronbach's alpha is explained as, "a measure of internal consistency, which is how closely related a set of items are as a group. It is considered to be a measure of scale reliability" (UCLA, n.d.).

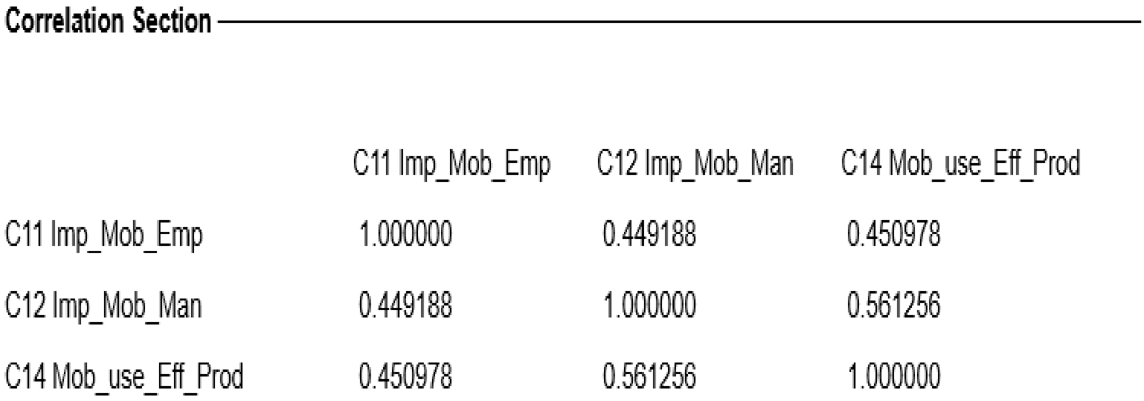
3.6.1 Validity

Validity entails the inspection of the information obtained for errors and inconsistencies, resulting in more confidence in the information obtained (Callegaro *et al.,* 2015:179).

3.6.1.1 Correlation analysis

Correlations were tested for variables pertaining to Section C, D, E and F to establish whether inter-item relationships exists, which are further discussed below.

SECTION C:



Correlation Section

	C11 Imp_Mob_Emp	C12 Imp_Mob_Man	C14 Mob_use_Eff_Prod
C11 Imp_Mob_Emp	1.000000	0.449188	0.450978
C12 Imp_Mob_Man	0.449188	1.000000	0.561256
C14 Mob_use_Eff_Prod	0.450978	0.561256	1.000000

Codes legend:

C11 Imp_Mob_Emp = Importance of Mobile Devices according to Employees.

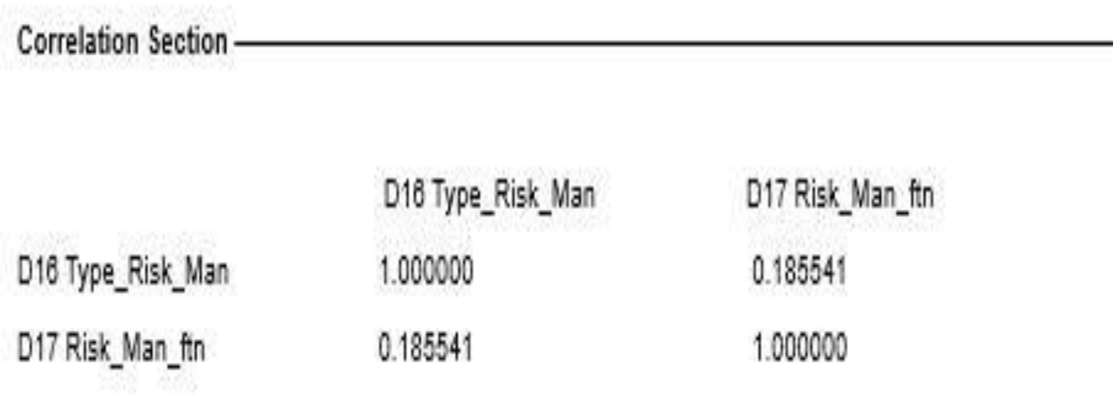
C12 Imp_Mob_Man = Importance of Mobile Devices according to Management.

C14 Mob_use_Eff_Pod = Use of Mobile Devices enhancing Efficiency and Productivity.

Interpretation:

- **C12 Imp_Mob_Man** have a medium positive correlation, with a value of 0.449, to **C11 Imp_Mob_Emp** (medium positive correlation = values between 0.40 to 0.69)
- **C14 Mob_use_Eff_Prod** have a medium positive correlation, with a value of 0.450, to **C11 Imp_Mob_Emp** (values between 0.40 to 0.69)
- **C14 Mob_use_Eff_Prod** have a medium positive correlation, with a value of 0.561, to **C12 Imp_Mob_Man** (values between 0.40 to 0.69)

SECTION D:



Correlation Section

	D16 Type_Risk_Man	D17 Risk_Man_ftn
D16 Type_Risk_Man	1.000000	0.185541
D17 Risk_Man_ftn	0.185541	1.000000

Codes legend:

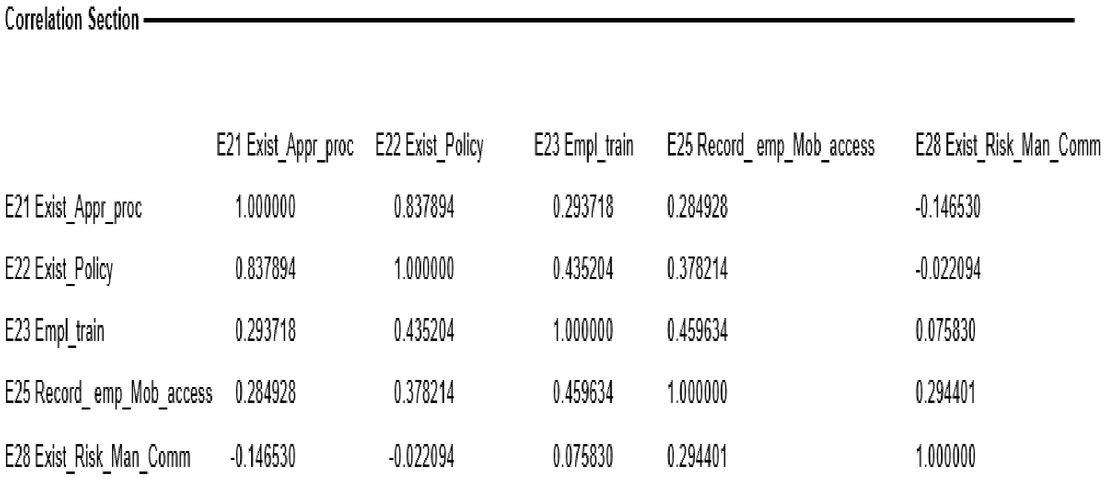
D16 Type_Risk_Man = Type of Risk Management system.

D17 Risk_Man_ftn = Existence of a Risk Management function.

Interpretation:

- **D17 Risk_Man_ftn** have a low positive correlation, with a value of 0.185, to **D16 Type_Risk_Man** (low positive correlation = values between 0 to 0.39).

SECTION E:



Correlation Section

	E21 Exist_Appr_proc	E22 Exist_Policy	E23 Empl_train	E25 Record_ emp_Mob_access	E28 Exist_Risk_Man_Comm
E21 Exist_Appr_proc	1.000000	0.837894	0.293718	0.284928	-0.146530
E22 Exist_Policy	0.837894	1.000000	0.435204	0.378214	-0.022094
E23 Empl_train	0.293718	0.435204	1.000000	0.459634	0.075830
E25 Record_ emp_Mob_access	0.284928	0.378214	0.459634	1.000000	0.294401
E28 Exist_Risk_Man_Comm	-0.146530	-0.022094	0.075830	0.294401	1.000000

Codes legend:

E21 Exist_Appr_proc = Existence of an approval process pertaining to mobile devices.

E22 Exist_Policy = Existence of a formal policy/procedure pertaining to mobile devices.

E23 Empl_train = Formal training provided to employees.

E25 Record-emp_Mob_access = Records of employees with mobile device access.

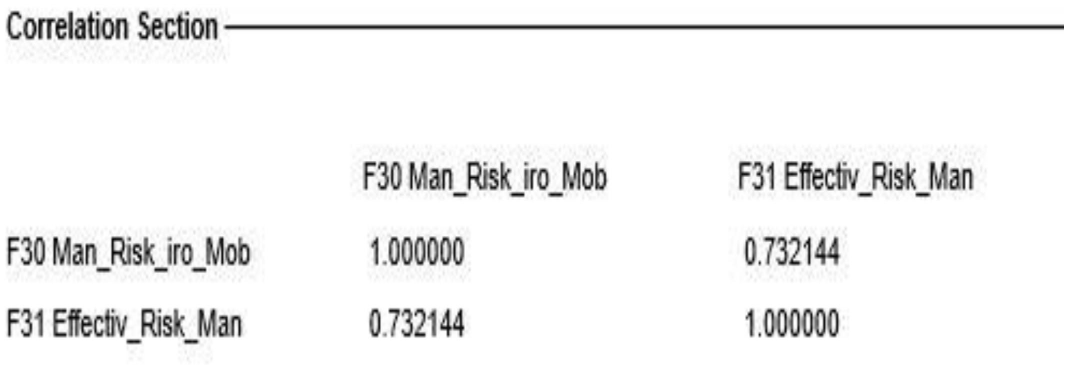
E28 Exist_Risk_Man_Comm = Existence of a risk management committee.

Interpretation:

- **E22 Exist_Policy** have a high positive correlation, with a value of 0.838, to **E21 Exist_Appr_proc** (higher positive correlation = values between 0.70 to 0.89),
- **E23 Empl_train** have a low positive correlation, with a value of 0.294, to **E21 Exist_Appr_proc** (values between 0 to 0.39),
- **E25 Record_emp_Mob_access** have a low positive correlation, with a value of 0.285, to **E21 Exist_Appr_proc** (values between 0 to 0.39),
- **E28 Exist_Risk_Man_Comm** have a low negative correlation, with a value of -0.147, to E21 Exist_Appr_proc (low negative correlation = values between 0 to -0.39),
- **E23 Empl_train** have a medium positive correlation, with a value of 0.435, to **E22 Exist_Policy** (values between 0.40 to 0.69),

- **E25 Record_emp_Mob_access** have a low positive correlation, with a value of 0.378, to **E22 Exist_Policy** (values between 0 to 0.39),
- **E28 Exist_Risk_Man_Comm** have a low negative correlation, with a value of -0.022, to **E22 Exist_Policy** (values between 0 to -0.39),
- **E25 Record_emp_Mob_access** have a medium positive correlation, with a value of 0.460, to **E23 Empl_train** (values between 0.40 to 0.69),
- **E28 Exist_Risk_Man_Comm** have a low positive correlation, with a value of 0.076 to **E23 Empl_train** (values between 0 to 0.39),
- **E28 Exist_Risk_Man_Comm** have a low positive correlation, with a value of 0.294 to **E25 Record_emp_Mob_access** (values between 0 to 0.39).

SECTION F:



Correlation Section

	F30 Man_Risk_iro_Mob	F31 Effectiv_Risk_Man
F30 Man_Risk_iro_Mob	1.000000	0.732144
F31 Effectiv_Risk_Man	0.732144	1.000000

Codes legend:

F30 Man_Risk_iro_Mob = Management of risks pertaining to mobile devices.

F31 Effectiv_Risk_Man = Effectiveness of Risk Management.

Interpretation:

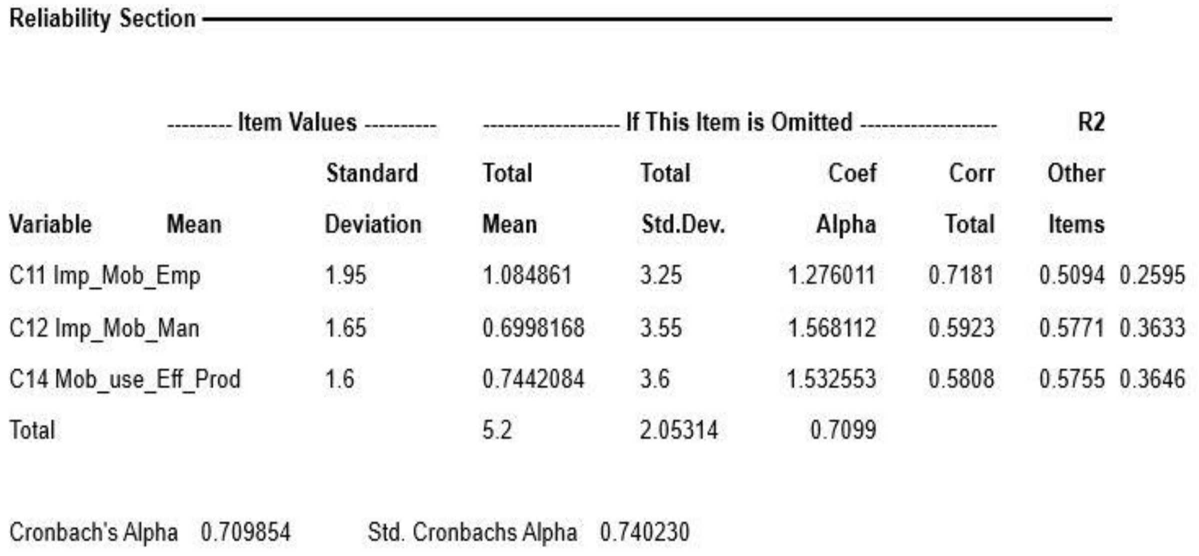
- **F30 Man_Risk_iro_Mob** have a high positive correlation, with a value of 0.732, to **F31 Effectiv_Risk_Man** (values between 0.70 to 0.89).

3.6.2 Reliability

Collis and Hussey (2014:217) are of the opinion that “Reliability” relates to the accuracy of the results in an instance of the research being re-performed by another researcher.

The reliability of information was confirmed in the research, using the Cronbach's Alpha Coefficient. This scoring was performed for certain questions incorporated in the survey document, specifically pertaining to Sections C, D, E and F as below.

SECTION C:

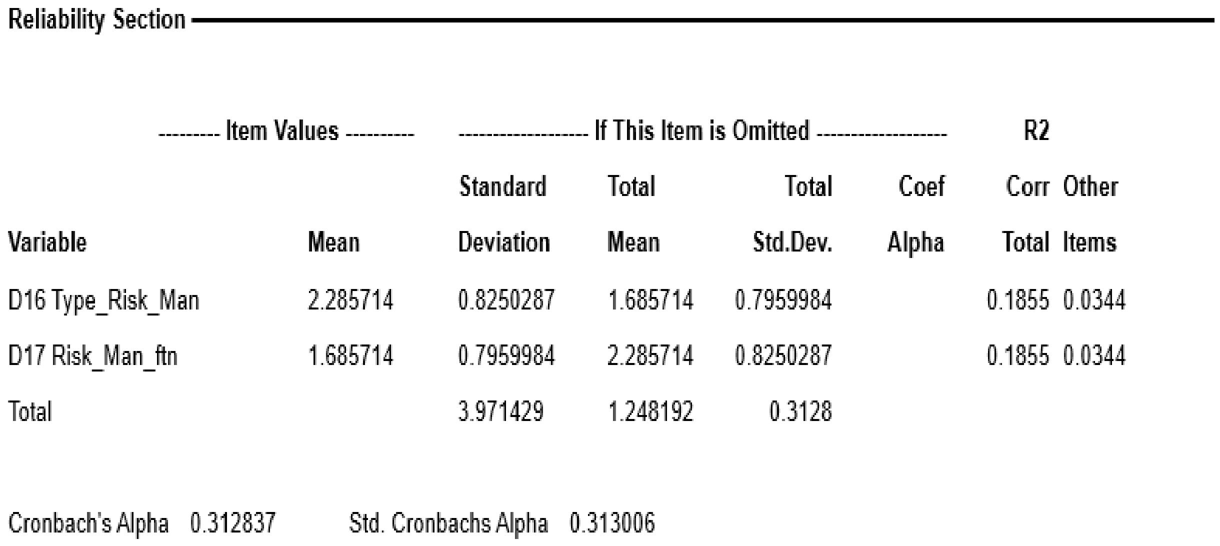


Reliability Section

	--------- Item Values ---------		------------------ If This Item is Omitted ------------------				R2	
		Standard	Total	Total	Coef	Corr	Other	
Variable	Mean	Deviation	Mean	Std.Dev.	Alpha	Total	Items	
C11 Imp_Mob_Emp		1.95	1.084861	3.25	1.276011	0.7181	0.5094	0.2595
C12 Imp_Mob_Man		1.65	0.6998168	3.55	1.568112	0.5923	0.5771	0.3633
C14 Mob_use_Eff_Prod		1.6	0.7442084	3.6	1.532553	0.5808	0.5755	0.3646
Total			5.2	2.05314	0.7099			

Cronbach's Alpha 0.709854 Std. Cronbachs Alpha 0.740230

SECTION D:

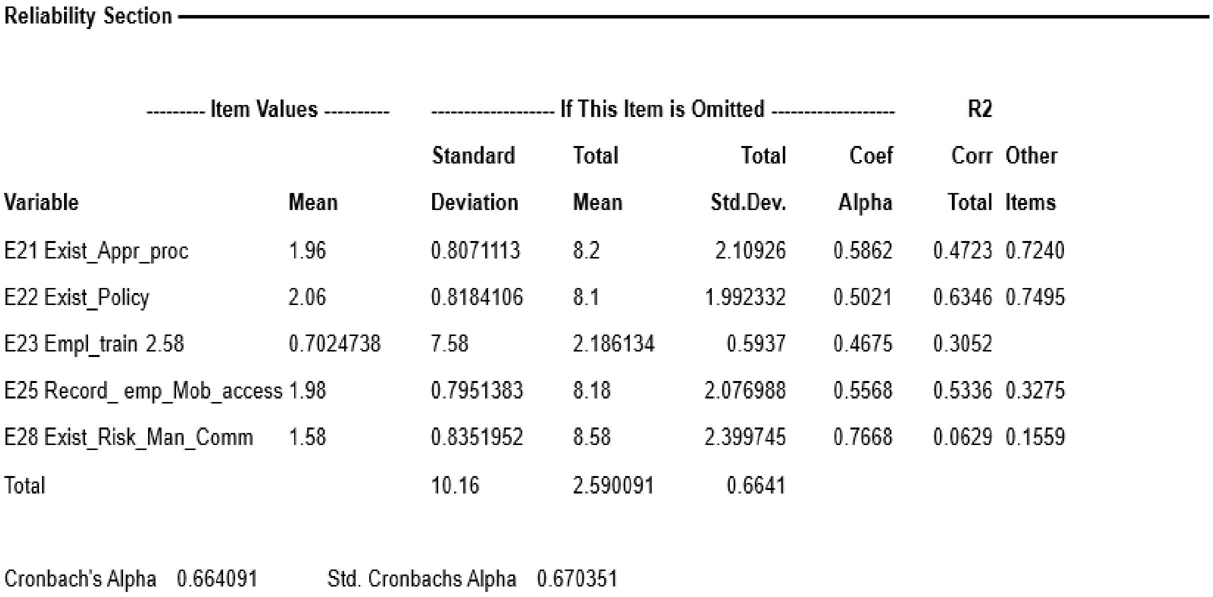


Reliability Section

	--------- Item Values ---------		------------------ If This Item is Omitted ------------------			R2	
		Standard	Total	Total	Coef	Corr	Other
Variable	Mean	Deviation	Mean	Std.Dev.	Alpha	Total	Items
D16 Type_Risk_Man	2.285714	0.8250287	1.685714	0.7959984		0.1855	0.0344
D17 Risk_Man_ftn	1.685714	0.7959984	2.285714	0.8250287		0.1855	0.0344
Total		3.971429	1.248192	0.3128			

Cronbach's Alpha 0.312837 Std. Cronbachs Alpha 0.313006

SECTION E:

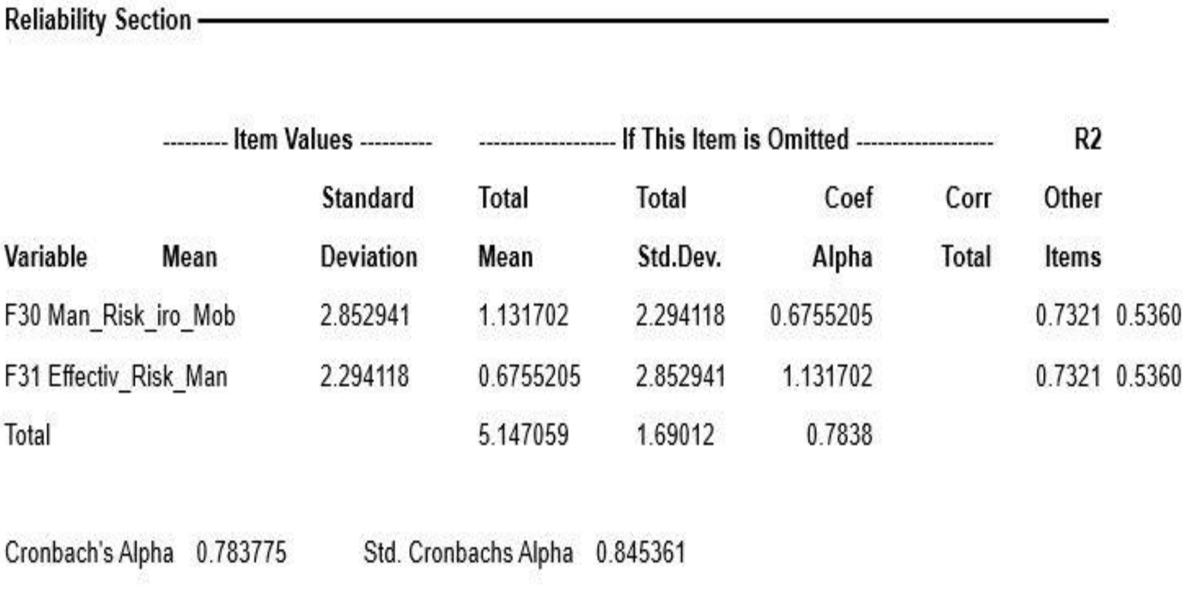


```
Reliability Section ________________________________________________________________

                 --------- Item Values ----------   ------------------ If This Item is Omitted ------------------   R2
                                         Standard      Total          Total      Coef      Corr  Other
Variable                     Mean        Deviation     Mean         Std.Dev.     Alpha     Total  Items
E21 Exist_Appr_proc          1.96        0.8071113     8.2           2.10926     0.5862    0.4723  0.7240
E22 Exist_Policy             2.06        0.8184106     8.1          1.992332     0.5021    0.6346  0.7495
E23 Empl_train 2.58          0.7024738     7.58          2.186134      0.5937    0.4675    0.3052
E25 Record_ emp_Mob_access 1.98          0.7951383     8.18         2.076988     0.5568    0.5336  0.3275
E28 Exist_Risk_Man_Comm      1.58        0.8351952     8.58         2.399745     0.7668    0.0629  0.1559
Total                                    10.16         2.590091       0.6641

Cronbach's Alpha   0.664091        Std. Cronbachs Alpha   0.670351
```

SECTION F:



```
Reliability Section ______________________________________________________

             --------- Item Values ----------   ------------------ If This Item is Omitted ------------------   R2
                                 Standard       Total          Total          Coef        Corr    Other
Variable          Mean           Deviation      Mean           Std.Dev.       Alpha       Total   Items
F30 Man_Risk_iro_Mob             2.852941       1.131702       2.294118       0.6755205           0.7321  0.5360
F31 Effectiv_Risk_Man            2.294118       0.6755205      2.852941       1.131702            0.7321  0.5360
Total                                           5.147059       1.69012        0.7838

Cronbach's Alpha   0.783775        Std. Cronbachs Alpha   0.845361
```

According to Gliem and Gliem (2003), an acceptable score is in excess of 0.7.

It was noted that statements tested in the two questions in Section D (D16 Type_Risk_Man and D17 Risk_Man_ftn) yielded a low Cronbach's alpha coefficient, and therefore it can be concluded that the scales included in these questions are not considered to be Likert-type. However, the level of alpha as depicted in the remaining items tested was consider to be acceptable for the majority of them, therefore the researcher proceeded with the performance of the data analysis.

3.7 Ethical considerations

According to Flick (2015:32), ethical issues such as voluntary participation should be clarified whilst performing the research project. The importance of ethical considerations during research is confirmed by Walliman (2011:47), indicating that the researcher should apply such when engaging with participants as well as when using the information gathered.

The following ethical considerations were included and shared with the participants:

i) Objectives of the research were explained to the participants;

ii) Minors were not included in the sample selected;

iii) Participants were informed that their participation was voluntary;

iv) Consent was obtained from the participants and they were informed that could withdraw from the study at any time without any implications;

v) Respondents were informed that the data collection instrument was a questionnaire to be answered;

vi) All information and data relating to the responses obtained during the research may be published, however, it will be a summarised version and not identifiable as a single respondent's information to ensure that anonymity of respondents is maintained; and

vii) Results of the research will be utilised for academic purposes only and may be published in an academic journal.

3.8 Limitations

The major limiting factors experienced during this study were:

i) Not receiving a written consent letter from the leadership of all entities, granting permission to the researcher to approach employees in their entities during the data collection/fieldwork phase; and

ii) Participants' daily work tasks took priority, delaying the completion and return of the questionnaire.

3.9 Chapter summary

This chapter discussed the research question, sub-questions and objectives, as well as the research design and methodology applied to the study. The process relating to the collection of data, assessment of the validity and reliability of responses received, as well as the analyses of such information was also discussed. The ethical considerations applied during the study were stated.

The analysis of the data and the results obtained are discussed in the next chapter, Chapter Four.

CHAPTER FOUR
DATA ANALYSIS AND RESULTS

4.1 Introduction

This chapter provides details and explanations relating to the information analysis and results obtained from the research performed, using a research questionnaire as a tool, focussing on local government entities located in the Namakwa District of the Northern Cape. The primary objectives are to ascertain the importance pertaining to the use of mobile devices for employees (senior management, management and non-management) of these entities in their practices to achieve organisational objectives, and the effectiveness of the entities' risk management processes in this regard.

The layout of this chapter is illustrated in Figure 4.1 below:

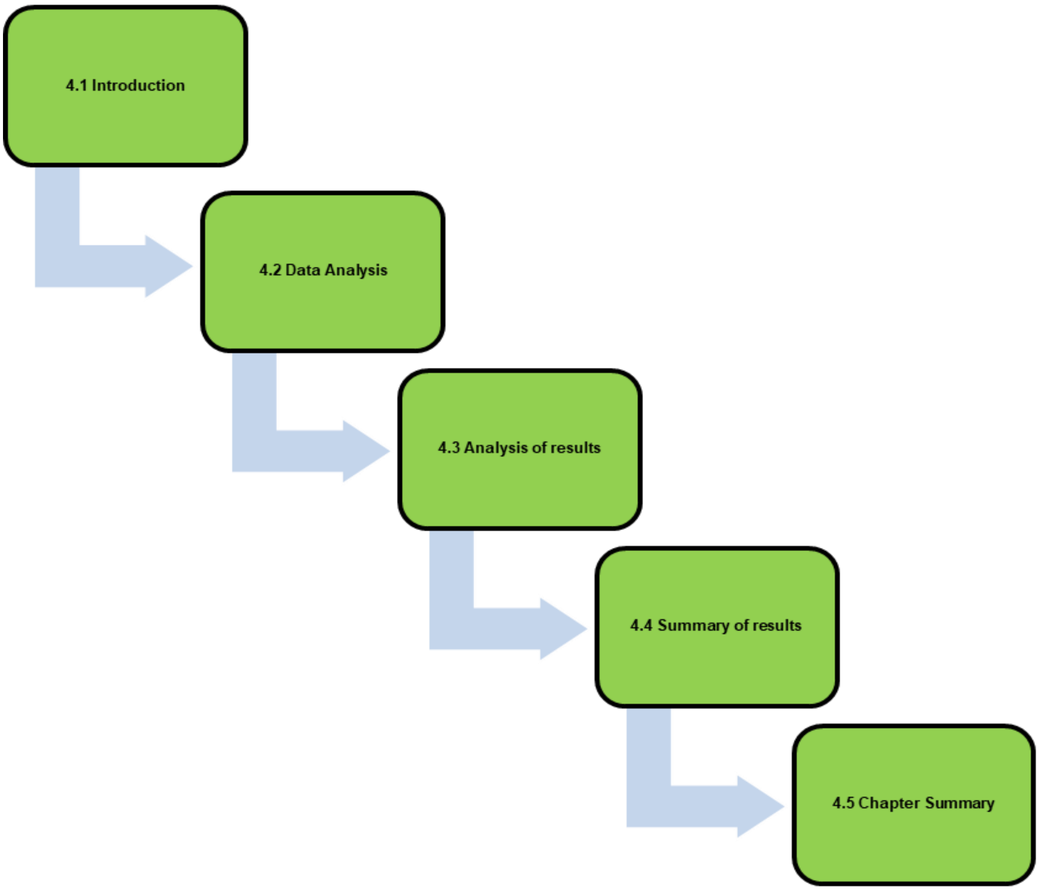


Figure 4.1: Layout of Chapter Four

4.2 Data analysis

4.2.1 Assistance received by the researcher

The researcher received assistance from a statistician in the data analysis process. This was performed to ensure that data analysis errors were not included in the final results presented in this report.

4.2.2 Sample

Non-probability sampling was applied. This specifically related to the convenience and snowball sampling approaches followed to collect information from local government entities in the Namakwa District of the Northern Cape. The targeted sample of respondents includes employees from the senior management, middle management and non-management groups in these entities.

4.2.3 Type of statistics utilised

Descriptive statistics were utilised to examine the data in this study. The reliability of information was assessed with Cronbach's Alpha Coefficient, whilst the validity of data was evaluated using correlation analysis as discussed in Chapter Three.

According to Saunders *et al.* (2016:534), correlation analysis is used to examine variables. The correlation analysis establishes the strength of a relationship between variables (Saunders *et al.,* 2016:534).

4.2.4 Data coding

According to Saunders *et al.* (2016:505), information obtained during the data collection phase is recorded in numerical codes, to ensure the performance of subsequent analysis is easier and more straightforward. Flick (2015:171) alluded to the fact that data coding refers to the allocation of numerical values to responses from research questionnaires obtained.

The data obtained were coded as per Appendix E, prior to the information being imported into the SPSS statistics software.

4.2.5 Information of participants

During the study, 51 research responses were received from participants. One respondent indicated that the completion of the research questionnaire document was not possible, as it was not within the person's ambit of work responsibilities. Therefore, this response was excluded from the analysis performed and the outcome was based on 50 completed questionnaires obtained from officials employed in these entities.

Information pertaining to the participants is contained in Table 4.1 below.

Table 4.1: Participant Information

Category		**Count**
Gender		
Valid	Male	32
	Female	18
	Total	50
Age category		
Valid	19 – 25	6
	26 – 35	17
	36 – 45	18
	46 – 55	8
	56 – 65	1
	Total	50
Level of seniority		
Valid	Senior Management	9
	Middle Management	16
	Non-Management	25
	Total	50

4.2.5.1 Descriptive results on participant information

Research Questionnaire – Section A: Gathered information on the enterprise and respondents, as illustrated below.

4.2.5.1.1 Demographics of respondents

A) Gender and age

Participants' gender is depicted in Table 4.2 and Figure 4.2, whilst age categories are shown in Table 4.3 and Figure 4.3.

Table 4.2: Gender

Gender	Count	Percentage	Cumulative Percentage
Male	32	64%	64%
Female	18	36%	100%
Total	50	100%	

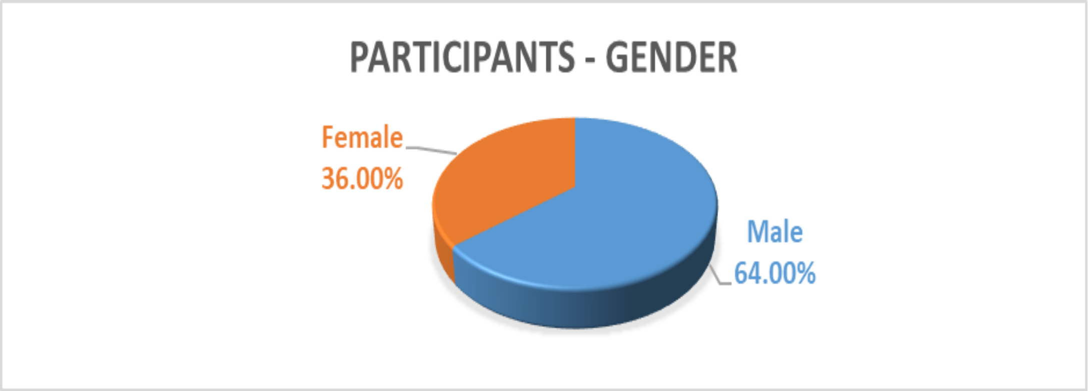


Figure 4.2: Gender

Table 4.3: Age

Respondent Information		Number of Respondents	Percentage	Cumulative Percentage
Age Categories	19 – 25	6	12%	12%
	26 – 35	17	34%	46%
	36 – 45	18	36%	82%
	46 – 55	8	16%	98%
	56 – 65	1	2%	100%
	Total	50	100%	

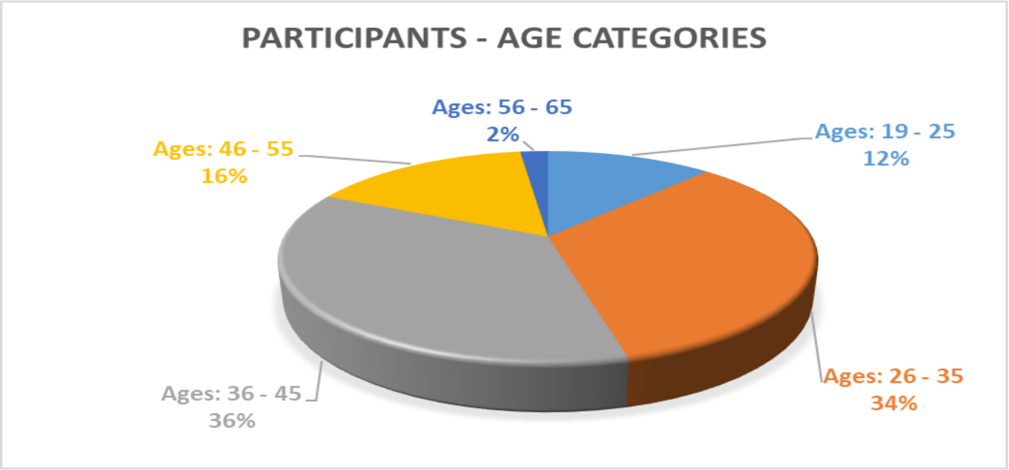


Figure 4.3: Age

Data relating to the study performed were obtained from participants in the local government entities in the Namakwa District of the Northern Cape. Data obtained from participants with 64% of the Male gender and 36% of the Female gender. Their age groups are summarised below:

- 12% age 19 – 25;
- 34% age 26 – 35;
- 36% age 36 – 45;
- 16% age 46 – 55; and
- 2% age 56 – 65.

B) Experience

Table 4.4: Average experience of the respondents

Position Level	**Average Years of Experience**
Senior Management	18.33 Years
Middle Management	15.85 Years
Non-Management	8.27 Years

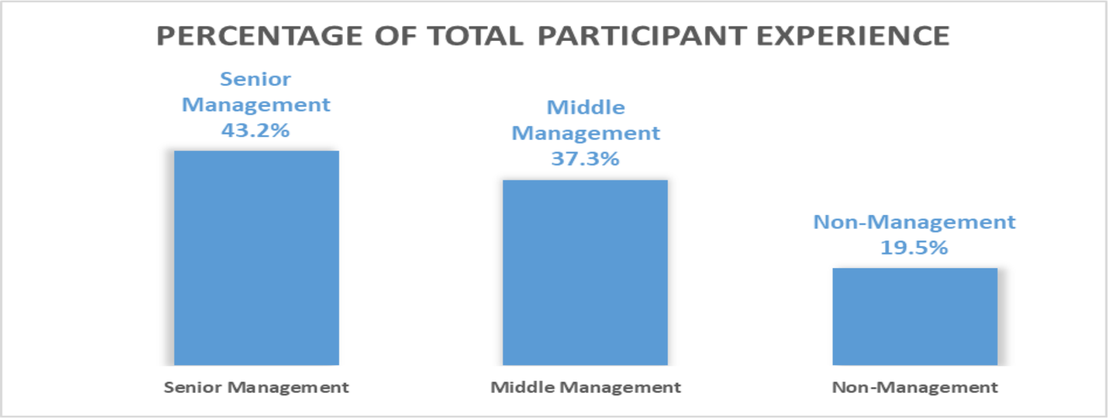


Figure 4.4: Respondents' average experience

Respondents include individuals in senior management with 18.33 years (experience) (equating to 43.20% of total years of experience of all respondents) on average, middle management with an average of 15.85 years (equating to 37.30%) and non-management with an average of 8.27 years (equating to 19.50%), as shown in Table 4.4 and Figure 4.4.

C) Levels of seniority

Table 4.5: Respondent's seniority level

Position Level	**Number**
Senior Management	9
Middle Management	16
Non-Management	25

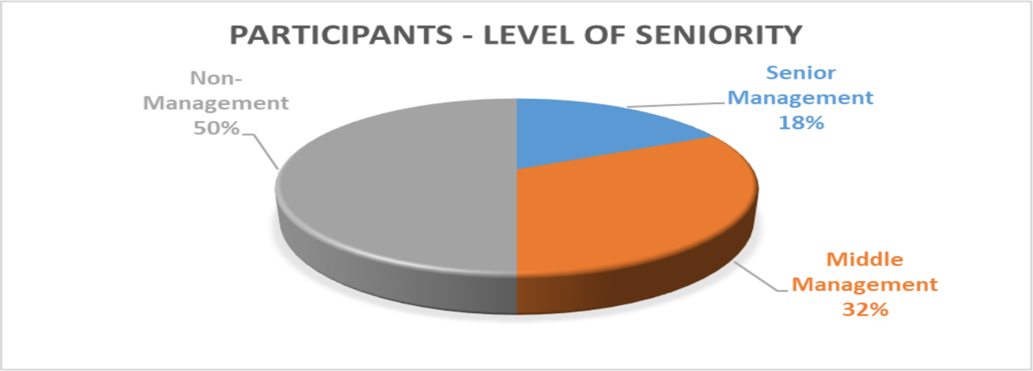


Figure 4.5: Level of seniority of respondents

Participants include individuals from all the different organisational position categories in the local government entities in the Namakwa District of the Northern Cape, as shown in Table 4.5 and Figure 4.5 above.

Level of seniority is summarised below:

- 18% (9 out of 50) from the senior management group,
- 32% (16 out of 50) from the middle management group, and
- 50% (25 out of 50) from the non-management group.

4.3 Analysis of results

The data collection window in the research process was closed on 31 July 2019. Research questionnaire were initially distributed via e-mail, whereafter multiple follow-ups (telephonic calls and e-mails) were performed between the period of June 2018 and July 2019. The analyses were performed and the outcome as depicted in Section 4.4 is based on completed questionnaires obtained from officials employed in these entities.

4.4 Summary of results

4.4.1 Introduction

This section provide explains the results relating to the effectiveness of risk management in the utilisation of mobile devices in local government entities in the Namakwa District of the Northern Cape. The outcome is based on 50 completed questionnaires obtained from officials employed in these entities.

Results are outlined in accordance with the research sub-questions previously stated in the introductory chapter.

4.4.2 Presentation of results based on research questions

4.4.2.1 Research question 1

Does management of local government entities in the Namakwa District of the Northern Cape, deem mobility of employees as important to achieve organisational objectives?

Research Questionnaire, Sections B and C, more specifically Questions 6, 7, 8, 9, 10, 12 and 14 gathered information relating to research question 1 and is presented below. The results included in this section pertaining to the analysis performed are utilised in answering the research question.

The details pertaining to these questions asked in the research questionnaire throughout the gathering of information to answer the research question is as follows:

- Does your organisation permit the connection of mobile devices to the enterprise’s network to access organisation’s information?
- Which mobile devices do you use?
- Are you allowed to access organisational information remotely when away from the office?
- How many years has your organisation been permitting the connection of mobile devices to the entity’s network?
- Does your organisation allow your personal mobile device to be connected to the enterprise’s network?
- Is the access with mobile devices deemed important by management to deliver on business objectives?
- Does the access of mobile devices to the corporate network enhance efficiency and productivity?

4.4.2.1.1 Entities allowing the use of mobile device connections to organisational networks

The majority of respondents (84%) indicated that their organisation used mobile devices, whilst 10% (5 out of 50) indicated that mobile devices are not utilised in their organisation. It was further noted that 6% (3 out of 50) indicated that they are not sure whether their organisations use mobile devices. Detailed results are shown in Table 4.6 and Figure 4.6 below.

Table 4.6: Use of mobile devices in organisation

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	42	84%	84%
Not sure	3	6%	90%
No	5	10%	100%
Total	50	100%	

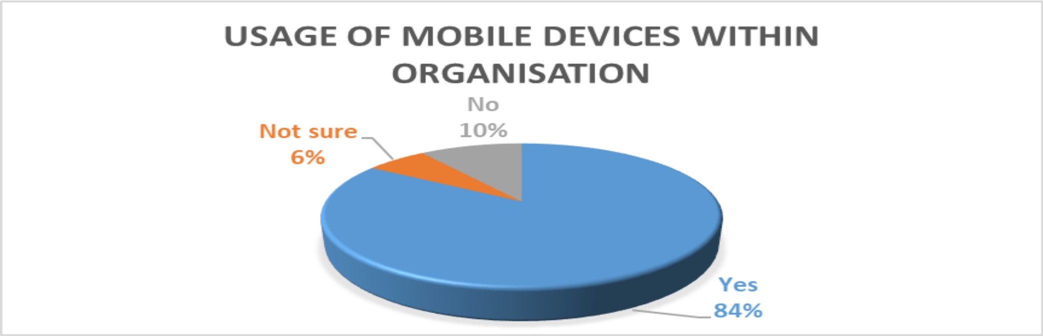


Figure 4.6: Entities using mobile devices

4.4.2.1.2 Types of mobile access allowed by the entities

As per Table 4.7 and Figure 4.7 below, the following was noted:

- 70.18% (40 out of 57) of responses confirm laptop use;
- 10.53% (6 out of 57) of responses confirm smart phones use;
- 17.54% (10 out of 57) of responses confirm tablet use; and
- 1.75% (1 out of 57) of respondents confirm the use of other devices.

Table 4.7: Types of mobile access allowed by entities

Types of Devices used	Number of Responses	Percentage
Laptops	40	70.18%
Mobile smartphones	6	10.53%
Tablets	10	17.54%
Other	1	1.75%
Total	57	100%

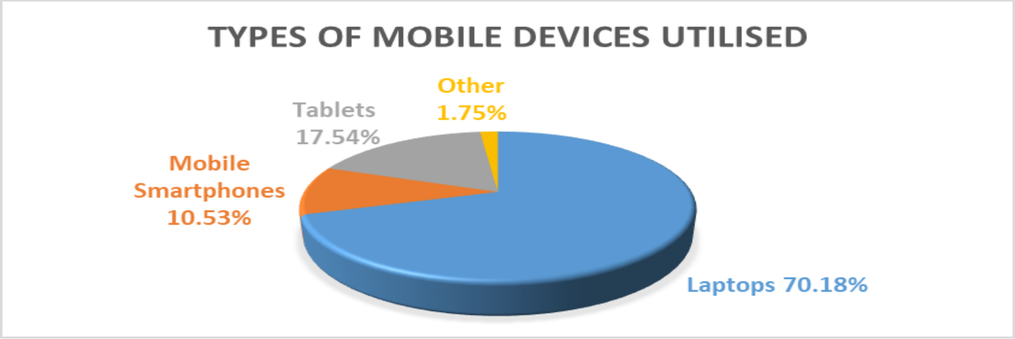


Figure 4.7: Types of access allowed with mobile devices by the entities

4.4.2.1.3 Mobile devices remotely utilised

More than half of all participants (58.54%) indicated that their organisation allows remote access with mobile devices, whilst 41.46% (17 out of 41) indicated that remote access with mobile devices was not allowed in their organisation.

Detailed results are depicted in Table 4.8 and Figure 4.8 below.

Table 4.8: Mobile devices remotely utilised by the entities

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	24	58.54%	58.54%
No	17	41.46%	100%
Total	41	100%	

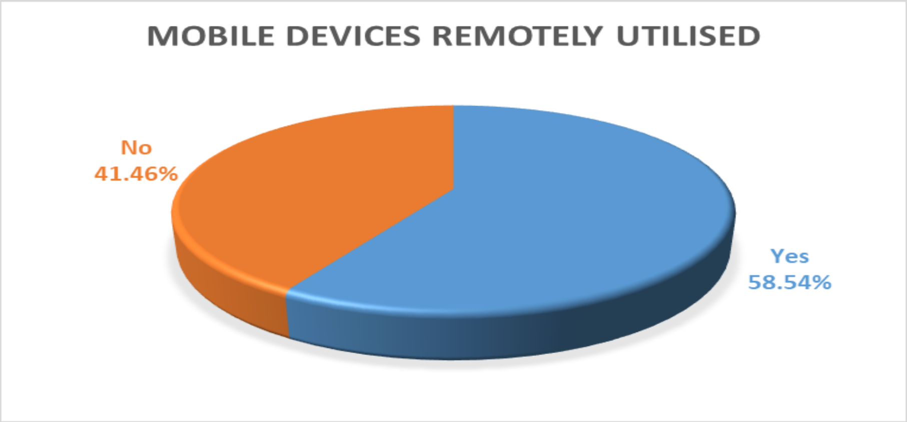


Figure 4.8: Mobile devices remotely utilised by the entities

4.4.2.1.4 Average number of years making use of mobile devices

Senior management indicate that on average their organisation has been using mobile devices for 8.67 years, whilst middle management has used it for 10.60 years on average. According to the non-management group, their organisation has been using these devices for an average of 5.00 years, as illustrated in Table 4.9 below.

Table 4.9: Average number of years the entities have used of mobile devices

Respondents' position level	Average years
Senior Management	8.67
Middle Management	10.6
Non-Management	5.0

4.4.2.1.5 Personal mobile devices allowed by the entities to connect to their network(s)

As shown in Table 4.10 and Figure 4.9 below, the permitting of personal mobile devices in entities is:

- 20.93% (9 out of 43) of respondents confirm the allowance of personal mobile devices use;
- 62.79% (27 out of 43) indicate it as not allowed; and
- 16.28% (7 out of 43) of respondents indicated that they are not sure whether their organisations allow the use of personal mobile devices.

Table 4.10: Use of personal mobile devices - Allowed

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	9	20.93%	20.93%
Not Sure	7	16.28%	37.21%
No	27	62.79%	100%
Total	43	100%	

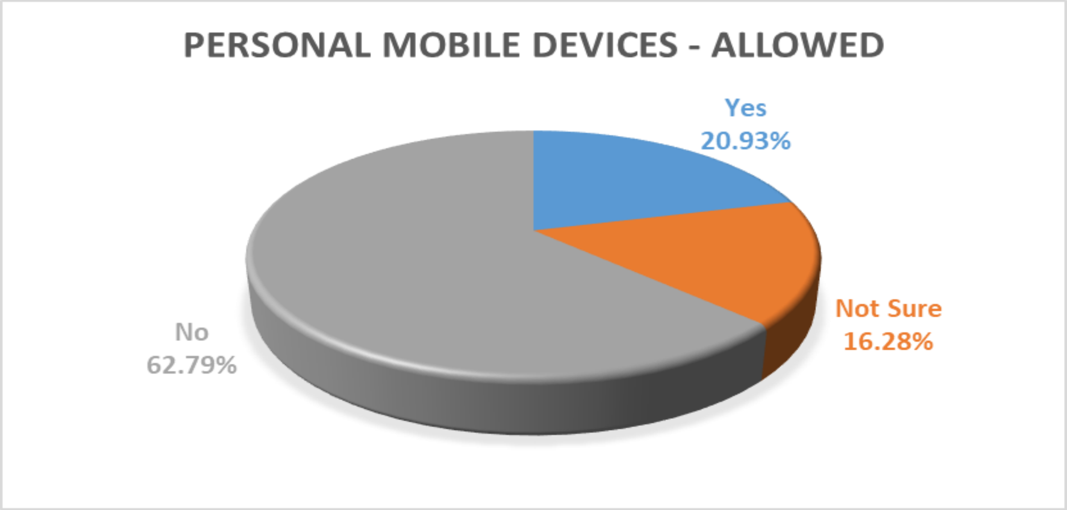


Figure 4.9: Use of personal mobile devices - Allowed

4.4.2.1.6 Importance of mobile device connections to the entity's network – Management

As illustrated in Table 4.11 and Figure 4.10 below, management deem the access of mobile devices in their organisations as very important, according to 39.58% (19 out of 48) of respondents, whilst 41.67% (20 out of 48) confirm it as important. However, 10.42% (5 out of 48) of respondents indicated it as not so important, whilst 8.33% (4 out of 48) indicated that their management deem it as not important at all.

Table 4.11: Importance of mobile devices: Management

Response	Number of Respondents	Percentage	Cumulative Percentage
Very Important	19	39.58%	39.58%
Important	20	41.67%	81.25%
Not so Important	5	10.42%	91.67%
Not Important at all	4	8.33%	100%
Total	48	100%	

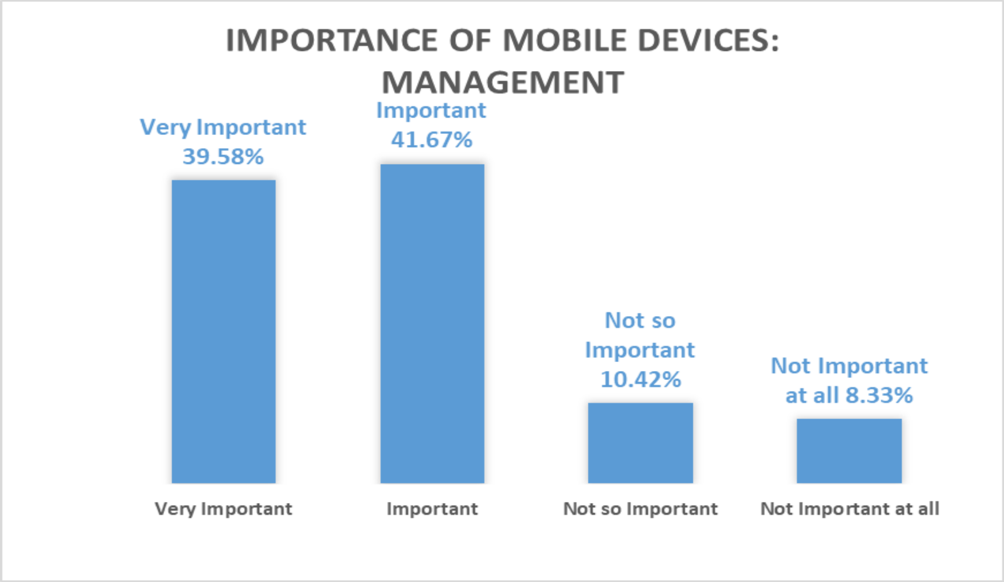


Figure 4.10: Importance of mobile devices - Management

4.4.2.1.7 Use of mobile devices enhances efficiency and productivity

According to the data analysed and shown in Table 4.12 and Figure 4.11 below, the following was noted:

- 52.50% (21 out of 40) of respondents strongly agree that the use of mobile devices enhances efficiency and productivity;
- 37.50% (15 out of 40) of respondents agree;
- 7.50% (3 out of 40) disagree; and
- 2.50% (1 out of 40) strongly disagree.

Table 4.12: Use of mobile devices enhances efficiency and productivity

Response	Number of Respondents	Percentage	Cumulative Percentage
Strongly Agree	21	52.50%	52.50%
Agree	15	37.50%	90%
Disagree	3	7.50%	97.50%
Strongly Disagree	1	2.50%	100%
Total	40	100%	

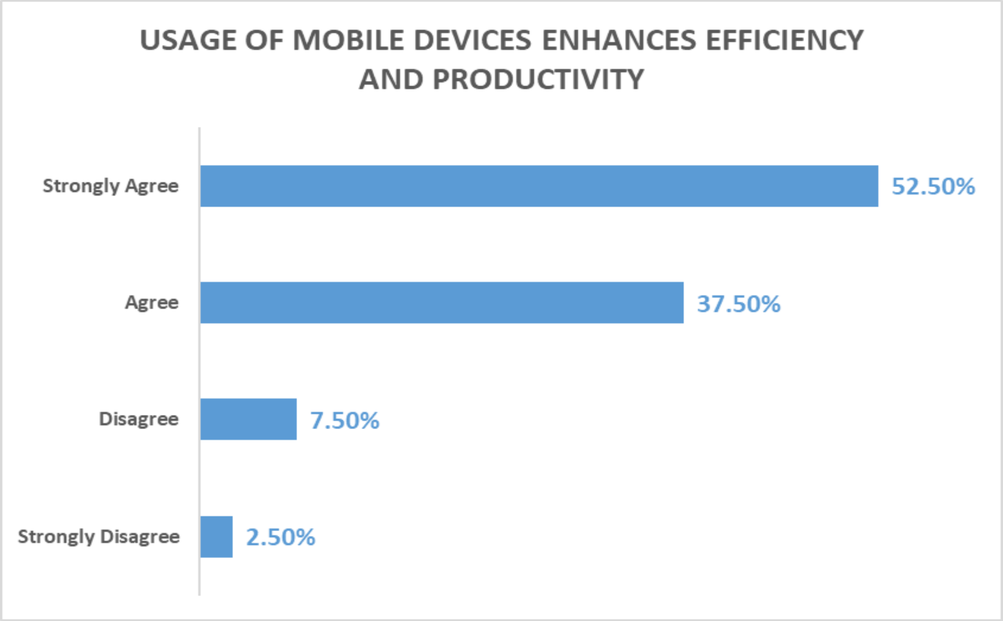


Figure 4.11: Use of mobile devices enhances efficiency and productivity

4.4.2.1.8 Summary

The majority of respondents indicated that their organisation make use of mobile devices, whilst the use of remote access with these devices were confirmed by just over half of participants. However, the majority of participants confirmed that their organisations do not allow the use of personal mobile devices. A substantial number of respondents confirmed that mobile devices are considered as important by their management, whilst 90% of respondents agree that mobile devices enhances their efficiency and productivity.

4.4.2.2 Research question 2

Do employees of local government entities in the Namakwa District of the Northern Cape deem connections with mobile devices to the entity's computer network(s) as necessary to deliver on organisational objectives?

Research questionnaire, Section C, more specifically questions 11 and 13 gathered information relating to research question 2, which is presented below. The results included in this section pertaining to the analysis performed, are utilised in answering the research question.

The details of these questions in the questionnaire to answer the research question are as follows:

- How important is access of your mobile device to the corporate network?
- How many hours per day on average do you spend on accessing business information on your enterprise's network using a mobile device?

4.4.2.2.1 Importance of mobile device connections to the entity's network - Employees

As can be seen from Table 4.13 and Figure 4.12 below, A total of 37.50% of responses confirmed that access with mobile devices is very important, and 27.08% (13 out of 48) indicated that the access with mobile devices is important. However, 16.67% (8 out of 48) of respondents indicated that the access with mobile devices is not so important, whilst 18.75% (9 out of 48) indicated it was not important at all.

Table 4.13: Importance of mobile devices: Employees

Response	Number of Respondents	Percentage	Cumulative Percentage
Very Important	18	37.50%	37.50%
Important	13	27.08%	64.58%
Not so Important	8	16.67%	81.25%
Not Important at all	9	18.75%	100%
Total	48	100%	

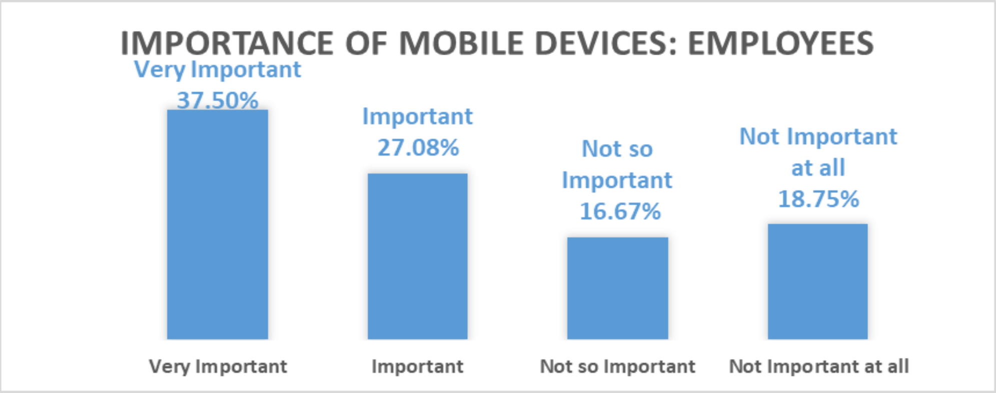


Figure 4.12: Importance of mobile devices – Employees

4.4.2.2.2 Time spent daily on average using mobile devices for business purposes

As illustrated in Table 4.14 below, the average time spent daily using mobile devices in these entities is as follows:

- Respondents in the senior management category indicated that they spent on average 5.88 hours daily using mobile devices;
- Respondents in the middle management category indicated that they spent on average 6.00 hours daily using mobile devices; and
- Respondents in the non-management category indicated that they spent on average 6.54 hours daily using mobile devices.

Table 4.14: Time spent on average daily using mobile devices

Respondent's Position Level	Average Hours Per Day
Senior Management	5.88
Middle Management	6.00
Non-Management	6.54

4.4.2.2.3 Summary

Based on the analysis of results pertaining to questions 11 and 13 included in the research tool utilised during data collection, the majority of respondents specified that access with mobile devices is important for them. It was also found that in excess of half of an employee’s workday is spent on the use of mobile devices, confirming the necessity of such devices in delivering on business objectives.

4.4.2.3 Research question 3

Does the risk exposure increase in instances where mobile device connection to the local government entities in the Namakwa District is permitted?

Research questionnaire, Section D, more specifically question 19, gathered information relating to research question 3, which is presented below. The results included in this section pertaining to the analysis performed are used in answering the research question.

- Has your organisation experienced a breach in terms of information security since permitting the use of mobile devices?

4.4.2.3.1 Experience of breaches in information security relating to mobile devices being utilised

Table 4.15: Experience of a breach in terms of information security since permitting mobile device connections

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	5	10.20%	10.20%
Not Sure	24	48.98%	59.18%
No	20	40.82%	100%
Total	49	100%	

Their organisations have experienced a breach in terms of information security since permitting connections with mobile devices, according to 10.20% (5 out of 49) respondents, whilst 40.82% (20 out of 49) indicated that their organisations have not experienced any information security breach. However, 48.98% (24 out of 49) of respondents indicated that they are not sure whether their organisations have experience an information security breach. Detailed results are depicted in Table 4.15 above.

4.4.2.3.2 Summary

Based on the analysis of results pertaining to question 19, it was noted that the risk exposure increased, as around 10% of respondents confirm that their organisations have experienced a breach in terms of information security since permitting connections of mobile devices.

4.4.2.4 Research question 4

Is risk management effectively performed in instances where mobile device connection to the network of local government entities in the Namakwa District is allowed?

Research questionnaire, Sections D, E and F, more specifically questions 15, 17, 18, 21, 22, 23, 25, 26, 27, 28, 29, 30 and 31 gathered information relating to Research Question 4 and is presented below. The results included in this section pertaining to the analysis performed, are utilised in answering the research question.

The details pertaining to these questions in the questionnaire to answer the research question are:

- Does your organisation have a risk management system?
- Does your organisation have a risk management function?
- What type of risk management function (in-house, outsourced or co-sourced) is it?
- Does your organisation have a formal process in place in terms of the approval of access requests pertaining to the connection of mobile devices to the enterprise’s network?
- Does your organisation have a formal policy/procedure developed to guide employees where mobile devices are utilised?
- Does your organisation provide formal training on a frequent basis to employees on mobile devices to create security awareness?
- Does your organisation maintain formal records of all employees approved to have access with mobile devices?
- How often does your organisation evaluate whether such access is still a requirement in line with the initial approval?
- How often are risk registers updated in your organisation?
- Does your organisation have a risk management committee?
- How often does the risk management committee meet?
- How good is the management of risks pertaining to mobile device use?

- How effective is risk management in your enterprise?

4.4.2.4.1 Risk management system is in place for the entities

A significant number of responses (67.34%) confirm the existence of a risk management system in their entities, whilst 18.37% (9 out of 49) indicated their organisation does not have a risk management system. However, 14.29% (7 out of 49) indicated that they are not sure whether their organisation does have a risk management system. Detailed results are depicted in Table 4.16 and Figure 4.13 above.

Table 4.16: Existence of a risk management system

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	33	67.34%	67.34%
Not Sure	7	14.29%	81.63%
No	9	18.37%	100%
Total	49	100%	

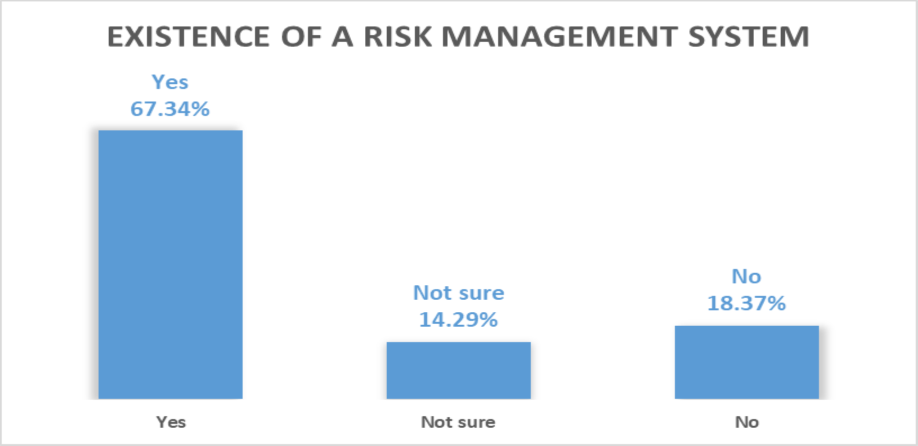


Figure 4.13: Existence of a risk management system

In 8 out of 35 (22.86%) instances, participants indicated that their organisation does have an electronic risk management system, whilst 18 out of 35 (51.43%) indicated that their organisation does not have such a system. However, 9 out of 35 (25.71%) indicated that they are not sure whether their organisation does have an electronic risk management system. Detailed results are depicted in Table 4.17 below.

Table 4.17: Electronic risk management system

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	8	22.86%	22.86%
Not Sure	9	25.71%	48.57%
No	18	51.43%	100%
Total	35	100%	

4.4.2.4.2 Risk management function exists for the entities

In 40.82% (20 out of 49) of participants pointed out that their organisation does have a risk management function, whilst 22.45% (11 out of 49) indicated that their organisation does not have such a function. However, 36.73% (18 out of 49) of respondents indicated that they are not sure whether their organisation does have a risk management function.

Detailed results are depicted in Table 4.18 and Figure 4.14 below.

Table 4.18: Existence of a risk management function

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	20	40.82%	40.82%
Not Sure	18	36.73%	77.55%
No	11	22.45%	100%
Total	49	100%	

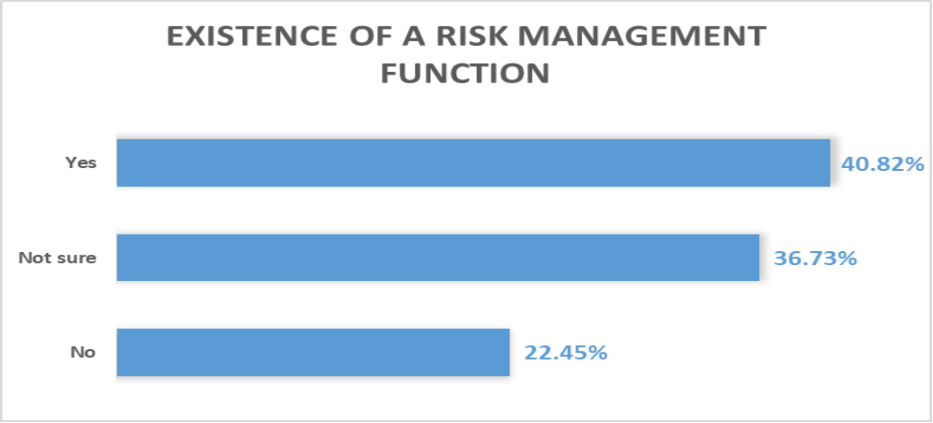


Figure 4.14: Existence of a risk management function

4.4.2.4.3 Types of risk management functions in place relating to the entities

As per Table 4.19 and Figure 4.15 below, the following was noted relating to the type of risk management functions:

- 53.33% (16 out of 30) of participants confirmed that their organisations have an in-house risk management function;
- 6.67% (2 out of 30) confirms a co-sourced risk management function;
- 6.67% (2 out of 30) confirms an outsourced risk management function; and
- 33.33% (10 out of 30) of respondents indicated that they are not sure as to which type of risk management function their organisation has.

Table 4.19: Type of risk management function

Response	Number of Respondents	Percentage	Cumulative Percentage
In-house	16	53.33%	53.33%
Co-sourced	2	6.67%	60%
Outsourced	2	6.67%	66.67%
Not Sure	10	33.33%	100%
Total	30	100%	

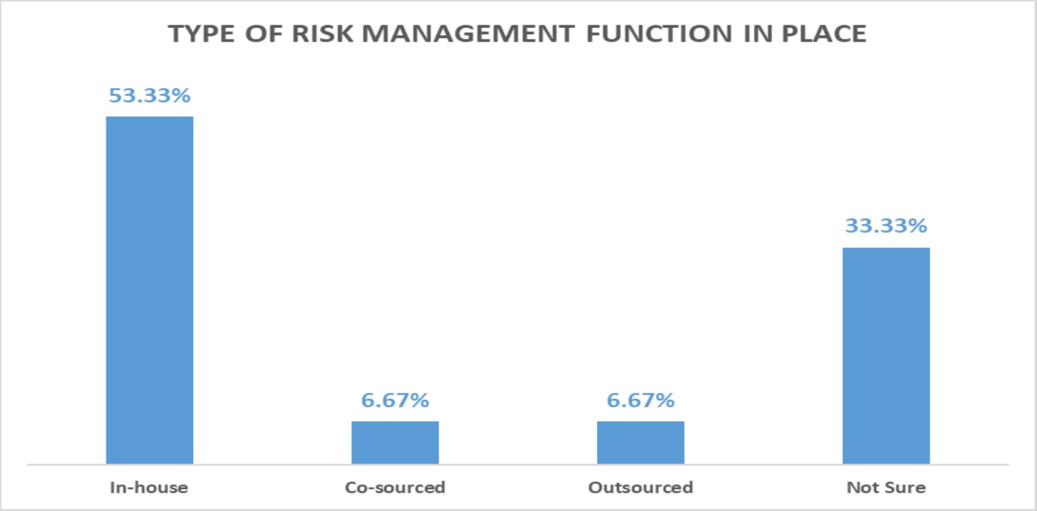


Figure 4.15: Type of risk management function

4.4.2.4.4 Existence of an approval process pertaining to mobile device connections to the enterprise's network

Their organisation has a formal process in place on the approval of access requests pertaining to the use of mobile devices, according to 17 out of 50 (34%) of respondents, whilst 15 out of 50 (30%) respondents indicated that their organisation does not have such a process. However, 18 out of 50 (36%) indicated that they are not sure whether their organisation has such a process.

Detailed results are depicted in Table 4.20 and Figure 4.16 below.

Table 4.20: Existence of an approval process pertaining to mobile device connections

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	17	34%	34%
Not Sure	18	36%	70%
No	15	30%	100%
Total	50	100%	

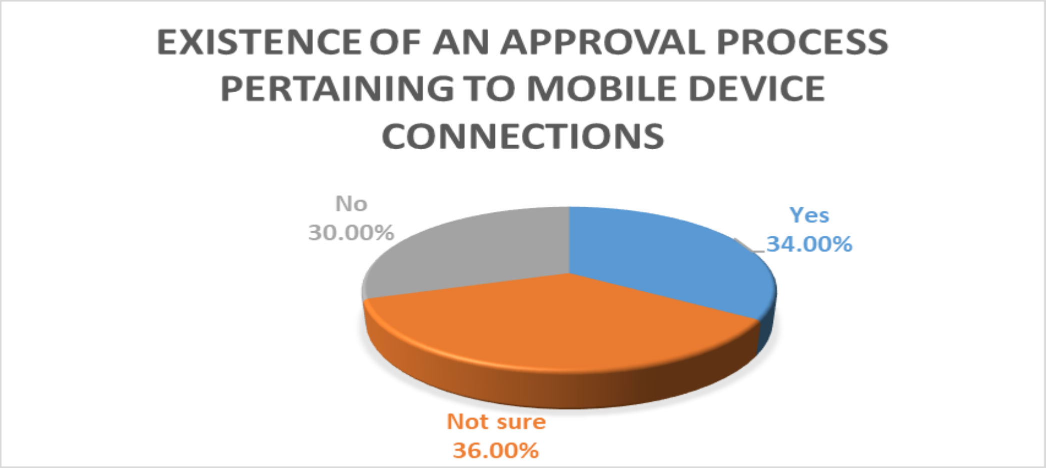


Figure 4.16: Existence of approval processes pertaining to mobile devices

4.4.2.4.5 Existence of guidance documents (policy and/or procedure) for employees pertaining to the use of mobile devices connected to enterprise network

In 15 out of 50 (30%) instances, participants confirmed that their organisation has formal policies and/or procedures in place pertaining to mobile devices, and 18 out of

50 (36%) indicated that their organisation does not have formal policies and/or procedures in place. However, 17 out of 50 (34%) confirmed that they are not sure.

Detailed results are depicted in Table 4.21 and Figure 4.17 above.

Table 4.21: Existence of policies and/or procedures pertaining to mobile devices

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	15	30%	30%
Not Sure	17	34%	64%
No	18	36%	100%
Total	50	100%	

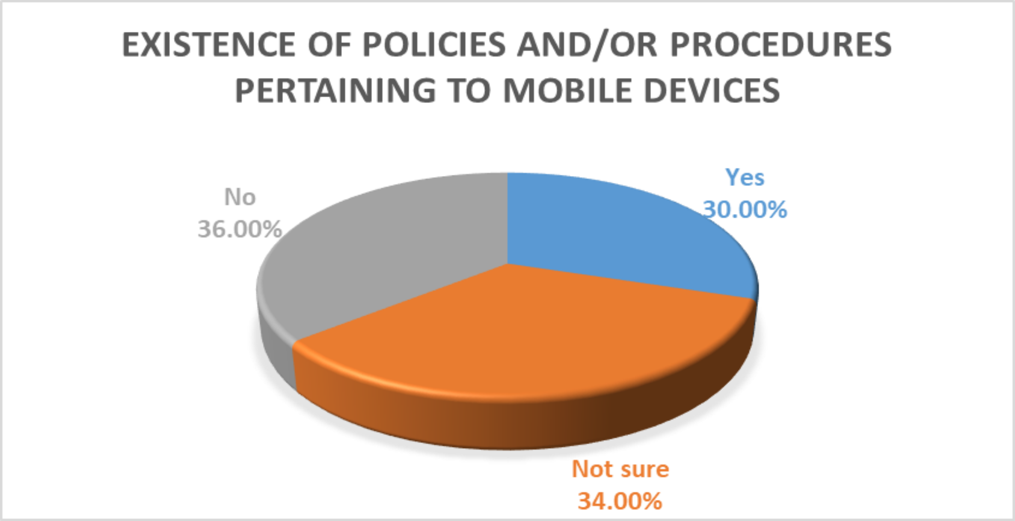


Figure 4.17: Existence of policies and/or procedures pertaining to mobile devices

4.4.2.4.6 Training provided in instances where mobile devices are utilised by entities

Training is provided in the organisations on mobile devices, according to a small number of respondents (12%), whilst a substantial number (70%) specified that formal training is not provided. However, 18% of respondents indicated that they are not sure whether their organisations provide formal training on mobile devices. Detailed results are depicted in Table 4.22 and Figure 4.18 below.

Table 4.22: Frequent training provided in instances where mobile devices are utilised

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	6	12%	12%
Not Sure	9	18%	30%
No	35	70%	100%
Total	50	100%	

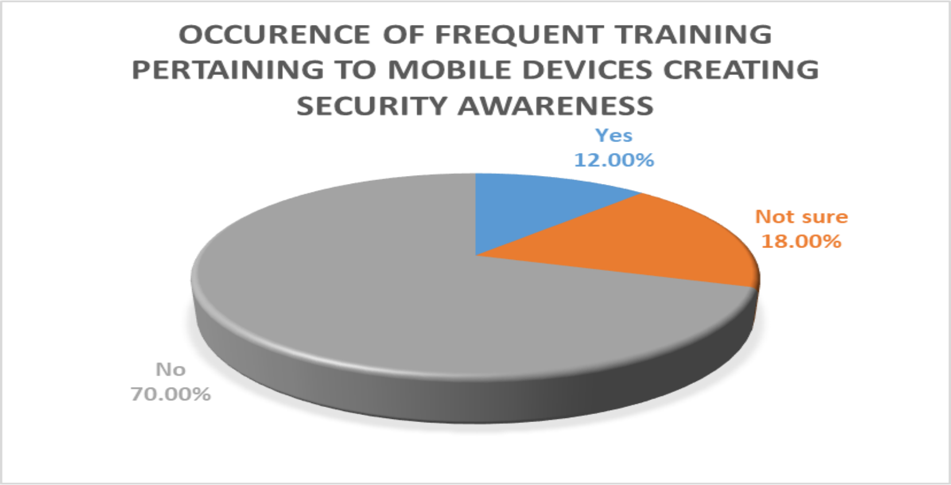


Figure 4.18: Frequent training provided in instances where mobile devices are utilised

4.4.2.4.7 Maintenance of formal records of employees with access to the organisation’s network with mobile devices

Formal records are maintained in their organisations pertaining to the use of mobile devices, according to 16 out of 50 (32%) respondents, whilst 15 out of 50 (30%) indicate that such records are not maintained. However, 19 out of 50 (38%) indicated that they are not sure whether their organisation maintain formal records pertaining to the use of mobile devices. Detailed results are depicted in Table 4.23 and Figure 4.19 below.

Table 4.23: Maintenance of records: Employees with mobile device access

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	16	32%	32%
Not Sure	19	38%	70%
No	15	30%	100%
Total	50	100%	

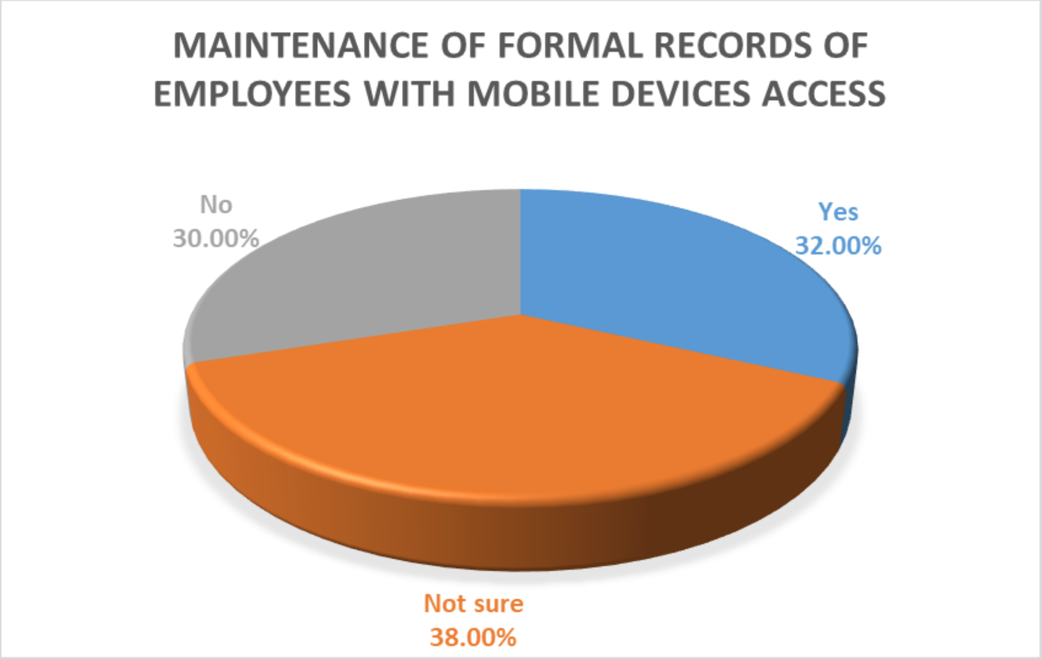


Figure 4.19: Maintenance of records - Employees with mobile device access

4.4.2.4.8 Frequency of re-evaluation of employees to determine relevance and requirements of mobile device connections to the organisation’s network

As per Table 4.24 and Figure 4.20 below, the following was noted relating to the evaluation of mobile device access:

- 20%% (4 out of 20) of respondents confirmed that their organisations assess the relevance of mobile device access on a monthly basis;
- 15% (3 out of 20) of participants confirmed that their organisations assess the relevance of mobile device access on a quarterly basis;
- 5% (1 out of 20) of participants confirmed that their organisations assess the relevance of mobile device access twice a year; and
- 60% (12 out of 20) of respondents indicated that they are not sure.

Table 4.24: Frequency of re-evaluation of mobile device users

Response	Number of Respondents	Percentage	Cumulative Percentage
Monthly	4	20%	20%
Quarterly	3	15%	35%
Twice a year	1	5%	40%
Not sure	12	60%	100%
Total	20	100%	

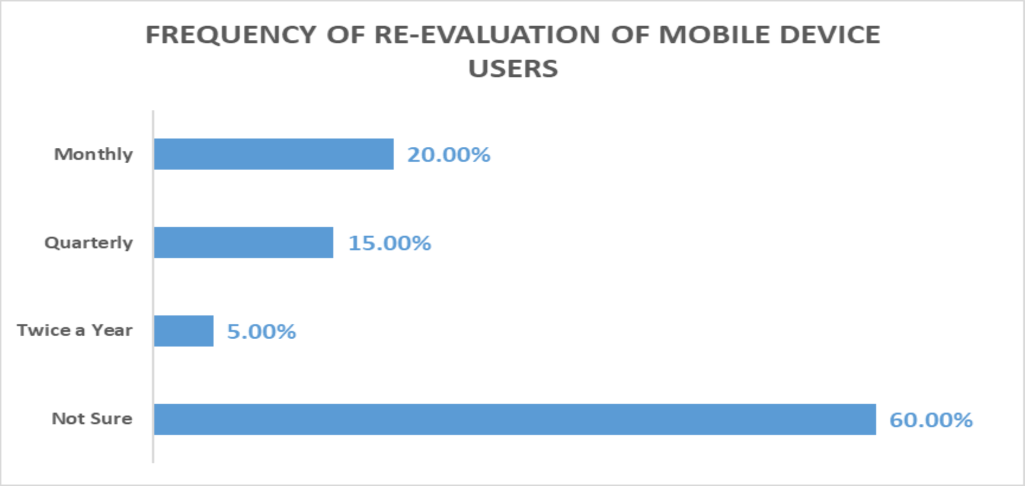


Figure 4.20: Frequency of re-evaluation of mobile device users

4.4.2.4.9 Frequency of updating risk registers in the entity

As per Table 4.25 and Figure 4.21 below, the following was noted relating to the updating of risk registers:

- 6.12% (3 out of 49) of participants indicated that their organisations update risk registers on a monthly basis;
- 51.02% (25 out of 49) confirm quarterly updating;
- 2.04% (1 out of 49) confirm updating twice a year;
- 12.24% (6 out of 49) confirm updating on an annual basis; and
- 28.57% (14 out of 49) of respondents indicated that they are not sure.

Table 4.25: Frequency of updating risk register

Response	Number of Respondents	Percentage	Cumulative Percentage
Monthly	3	6.12%	6.12%
Quarterly	25	51.02%	57.14%
Twice a year	1	2.04%	59.18%
Annually	6	12.24%	71.43%
Not sure	14	28.57%	100%
Total	49	100%	

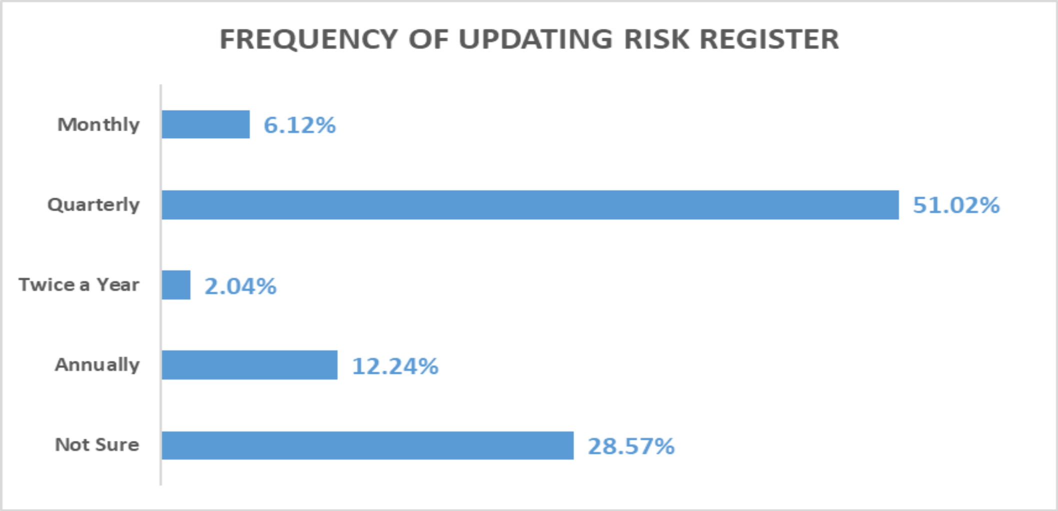


Figure 4.21: Frequency of updating risk register

4.4.2.4.10 Existence of a risk management committee where risk is discussed

Respondents in 64% (32 out of 50) instances indicated that their organisation does have a risk management committee, whilst 22% (11 out of 50) indicated that their organisation does not have such a committee. However, 14% (7 out of 50) indicated that they are not sure. Detailed outcomes are depicted in Table 4.26 and Figure 4.22 below.

Table 4.26: Existence of a risk management committee

Response	Number of Respondents	Percentage	Cumulative Percentage
Yes	32	64%	64%
Not Sure	7	14%	78%
No	11	22%	100%
Total	50	100%	

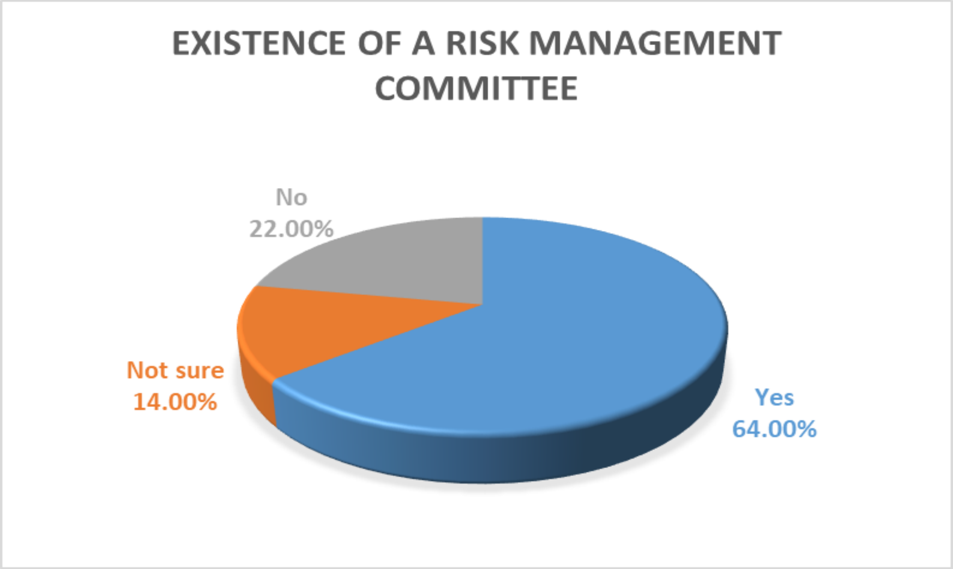


Figure 4.22: Existence of a risk management committee

4.4.2.4.11 Frequency of meetings by the risk management committee to discuss risks relevant to the business

- 4.88% (2 out of 41) of respondents indicated that their organisations risk management committee meets on a monthly basis to discuss risks;
- 60.98% (25 out of 41) confirmed the meeting on a quarterly basis;
- 4.88% (2 out of 41) confirmed the meeting on an annual basis; and
- 29.27% (12 out of 41) of respondents indicated that they are not sure.

Detailed results are depicted in Table 4.27 and Figure 4.23 below.

Table 4.27: Frequency of risk management committee meetings

Response	Number of Respondents	Percentage	Cumulative Percentage
Monthly	2	4.88%	4.88%
Quarterly	25	60.98%	65.85%
Annually	2	4.88%	70.73%
Not sure	12	29.27%	100%
Total	41	100%	

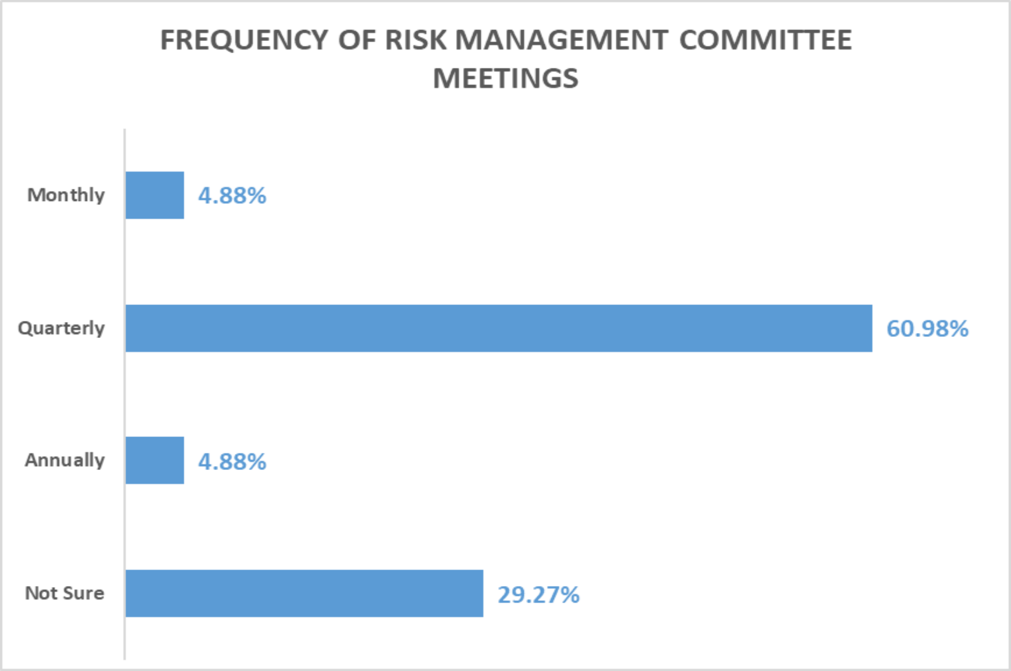


Figure 4.23: Frequency of risk management committee meetings

4.4.2.4.12 Risks relevant to mobile device connections are managed

As seen in Table 4.28 and Figure 4.24 below, 16.67% of respondents (6 out of 36) indicated that risks relating to mobile devices connected to their enterprise's network are managed very well (very good) and 19.94% (7 out of 36) confirmed it as good, whilst 27.78% (10 out of 36) of respondents indicated that risks relating to mobile devices connected to their enterprise's network are managed fairly good. However, 36.11% (13 out of 36) confirmed that these risks are poorly managed.

Table 4.28: Risks relevant to mobile device connections are managed

Response	Number of Respondents	Percentage	Cumulative Percentage
Very Good	6	16.67%	16.67%
Good	7	19.44%	36.11%
Fairly Good	10	27.78%	63.89%
Poor	13	36.11%	100%
Total	36	100%	

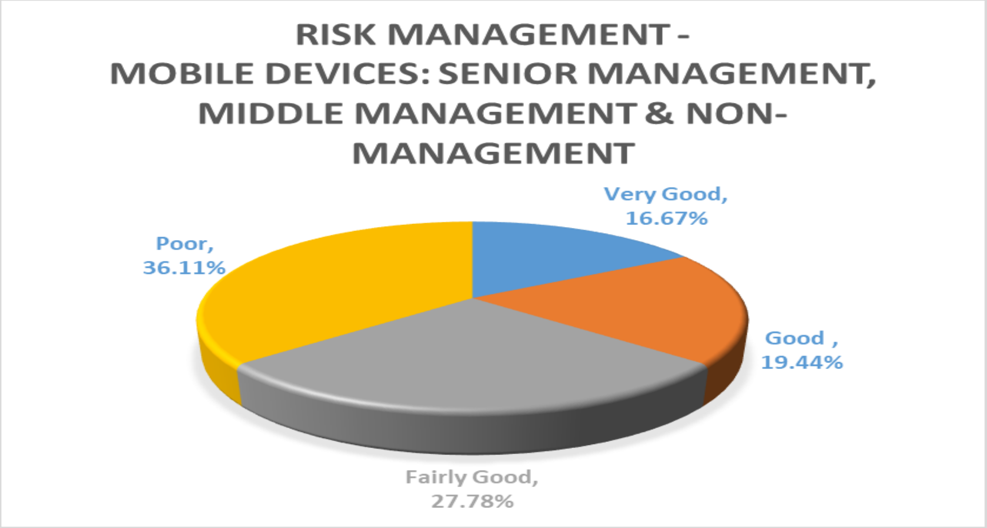


Figure 4.24: Risks relevant to mobile device connections are managed

4.4.2.4.13 Risk management in the enterprise is effective

As illustrated in Table 4.29 and Figure 4.25 below, the majority of respondents (60.98%) agree that the risk management in their organisation is effective, whilst 9.76% (4 out of 41) strongly agree. However, 26.83% (11 out of 41) of participants disagree that the risk management in their organisation is effective, whilst 2.44% (1 out of 41) strongly disagree.

Table 4.29: Risk management in the enterprise is effective

Responds	Number of Respondents	Percentage	Cumulative Percentage
Strongly Agree	4	9.76%	9.76%
Agree	25	60.98%	70.73%
Disagree	11	26.83%	97.56%
Strongly Disagree	1	2.44%	100%
Total	41	100%	

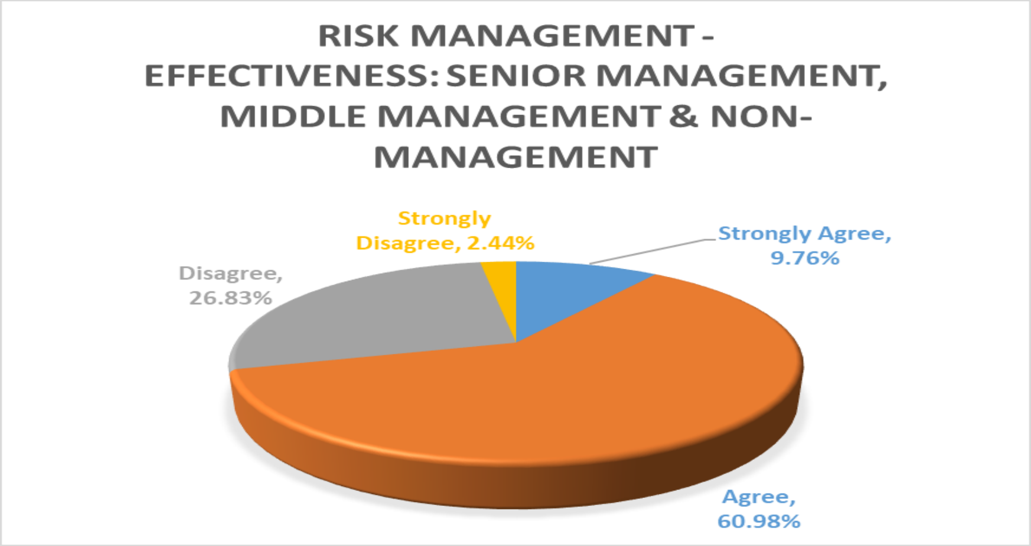


Figure 4.25: Risk management in the enterprise is effective

4.4.2.4.14 Summary

- A significant number of participants confirmed that their organisation does have a risk management system;
- In limited instances, participants indicated that their organisation does have an electronic risk management system;
- Less than half of participants indicated that their organisation does have a risk management function;
- A limited number of respondents is certain that their organisations have a formal process in place on the approval of access requests pertaining to the use of mobile devices;
- In limited instances, participants confirmed that their organisation has formal policies and/or procedures in place pertaining to mobile devices;

- A significant number of participants confirmed that formal training is not provided;
- Limited respondents confirm that formal records are maintained in their organisations pertaining to the use of mobile devices;
- The majority of participants confirmed that they are not sure whether initial mobile device access is re-evaluated periodically;
- The majority of respondents confirmed that their organisation does have a risk management committee;
- The majority of respondents are certain that their risk management committee is active;
- Respondents equating to 36.61% indicated that risks relating to mobile devices connected to their enterprise's network is satisfactorily (good) managed;
- The majority of participants agree that risk management in their organisation is effective.

4.4.3 Research questions revisited

Based on the results presented above, the following conclusions pertaining to the research questions were drawn.

Table 4.30: Research questions revisited: Conclusions

Research sub-question	Conclusion
Does management of local government entities in the Namakwa District of the Northern Cape, deem mobility of employees as important to achieve organisational objectives?	The use of mobile devices is important to the management of these entities, and enhances efficiency and productivity; impacting the achievement of organisational objectives. This was substantiated by the fact that: The majority of participants (in excess of 80%) confirm the importance of mobile devices according to their management in the accomplishment of organisational objectives; and A substantial number of participants (90%) confirm that the use of mobile devices enhances their efficiency and productivity.
Do employees of local government entities in the Namakwa District of the Northern Cape, deem connections with mobile devices to the entity's computer network(s) as necessary to deliver on organisational objectives?	The use of mobile devices is important to the employees of these entities, and enhances efficiency and productivity; impacting the achievement of organisational objectives. This was substantiated by the fact that: The majority of participants (in excess of 60%) confirm the importance of access with their mobile devices to the organisational network; and A substantial number of respondents (90%) confirm that the use of mobile devices enhances their efficiency and productivity.
Does the risk exposure increase in instances where mobile device connections to the local government entities in the Namakwa District is permitted?	Risk exposure increased, as around 10% of respondents confirm that their organisations have experienced a breach in terms of information security since permitting connections with mobile devices.
Is risk management effectively performed in instances where mobile device connections to the network of local government entities in the Namakwa District is allowed?	The risk management practices in these entities require improvement, more specifically relating to the following at an operational level: Improvement or establishment of risk management functions in these entities; Improvement in the risk management systems utilised with these entities;

	Improvement of employee Training and Awareness; Establishment, improvement or amendments to the Privacy and Security policy, Training and Awareness Procedure as well as the Risk Management Policy; Improvement of the control(s) pertaining to the recordkeeping of information regarding users with mobile device access; and Improvement relating to the re-evaluation process (on a periodic basis) pertaining to the mobile device users, ensuring that only valid and authorised users with proven requirements have access with these devices.

Discussion

The conclusions drawn from the above research questions indicate that:

- The majority of participants confirmed that their organisation make use of mobile devices, and a substantial number of respondents confirmed that mobile devices are considered important by themselves as well as their management, whilst 9 out of 10 respondents agree that mobile devices enhances their efficiency and productivity. These results confirm the statement of Shacklett (2016) who stipulated that the use of mobile devices became important in the modern business world and have an effect on productivity. It also corroborates the statement of Jamaluddin *et al.* (2015) who is of the opinion that the use of mobile devices by employees give them access to organisational information whilst away from the office, and therefore increase productivity. This is aligned to the conclusion by Sheldon (2013b) as well as Ludwig (2018), who indicated that the use of mobile devices impacts efficiency and productivity of employees.
- The majority of participants confirmed that their organisations does not allow the use of personal mobile devices. This conservative approach is followed to minimise the risk of information being accessed or altered by unauthorised individuals and is aligned to the opinions of Pillay *et al.* (2013) as well as Miller *et al.* (2012) and Hetting (2014), who all concluded that the utilisation of a strategy where employees' personal mobile devices are utilised poses a risk of information loss to the organisation. These results corroborate the statement of Siddiqui (2014), who stipulated that sensitive information might get lost or compromised where employees dispose of their devices, sharing it with family or in the event of them exiting the organisation.
- There is an increase in risk exposure, which is confirmed by the results as around 10% of respondents confirm that their organisations have experienced a breach in terms of information security since permitting connections with mobile devices. These results confirm the statement of Chen and Li (2017) who

concluded that information is at risk of being compromised whilst using mobile devices. The results also align with Kleiner and Disterer (2015) who concluded that the use of mobile devices currently top the list of security risks. The results further corroborate the statement of Ames *et al.* (2016), who are of the opinion that information stored on mobile devices are at risk of compromise where suitable security is not considered or put in place.

- Risk management practices in these entities, specifically mitigation at an operational level, require improvement based on the results as per below:
- In limited instances, participants indicated that their organisation does have an electronic risk management system;
- Less than half of participants indicated that their organisation does have a risk management function;
- A limited number of respondents believe that their organisation has a formal process in place on the approval of access requests pertaining to the use of mobile devices;
- In limited instances, participants indicated that their organisation has formal policies and/or procedures in place pertaining to mobile devices;
- A significant number of participants confirmed that formal training is not provided;
- Limited respondents confirm that formal records are maintained in their organisations pertaining to the use of mobile devices;
- The majority of respondents indicated that they are not sure whether initial mobile device access is re-evaluated periodically;
- Respondents of 4 out of 10 indicated that risks relating to mobile devices connected to their enterprise’s network is satisfactorily managed;

The shortcomings in risk management as per the results above are confirmed as important areas requiring improvement. This was corroborated by conclusions drawn by other researchers pertaining to the significance of risk management (Siwangaza & Dubihlela, 2017), where mobile devices are utilised, as explained below:

- Hetting (2014) concluded that organisations require appropriate risk management, as the researcher stated that controls should be implemented to ensure that information does not land in the hands of unwanted individuals or groups;
- Vignesh and Asha (2015) concluded that access with mobile devices to organisational information should be restricted and only provided to employees based on seniority and job description;
- Souppaya and Scarfone (2013) confirm that access with mobile devices to organisational information should be defined;

- According to Gerba *et al.* (2015), organisations should develop and implement a privacy and security policy where mobile devices are utilised;
- Yevseyeva *et al.* (2014) concluded that a privacy and security policy should be complied with in the search of protection against security risks;
- Harris *et al.* (2013) are of the opinion that training and awareness of users is important;
- Siddiqui (2014) also confirms that user training is essential;
- Hanlin *et al.* (2013) are of the opinion that training and awareness will ensure that users would be more vigilant about security whilst utilising mobile devices; and
- Souppaya and Scarfone (2013) concluded that the recordkeeping of users with mobile device access and frequent re-evaluation of such access is good practice.

Based on the above discussions, it is evident that:

- Employees and management of local government entities in the Namakwa District consider the use of mobile devices as important and necessary in achievement of organisational objectives; and
- The risk management practices in these entities, specifically mitigation at an operational level, require improvement.

4.5 Chapter summary

This chapter presented the reader with the details and interpretations of the observations noted. The analysis and interpretation of the results were performed to enable the researcher to respond to the research questions as well as the research objectives. The composition of the sample was explained by using descriptive statistics. The outcomes were presented in accordance with the research questions previously discussed in this report.

The following chapter, Chapter Five, presents recommendations and the conclusions reached.

CHAPTER FIVE
DISCUSSION, RECOMMENDATIONS AND CONCLUSIONS

5.1 Introduction

It was established that the use of mobile devices is accommodated by the majority (84%) of local government entities in the Namakwa District of the Northern Cape, based on information obtained and analysed from respondents in this study. However, the mobile devices used in these entities are mostly laptops (70.18%), whilst minimum use of other mobile devices such as tablets (17.54%) and smart phones (10.53%) occurs. It was further found that the majority (72.73%) of smart phone and tablet users are senior officials (middle management and senior management).

Furthermore, it was found that these entities generally do not permit employees to utilise their personal mobile devices (62.79% of officials indicating that they are not allowed). Therefore, these entities generally still use the traditional approach of providing their employees with their specifically approved types of mobile devices (Corporate Owned Device strategy), and not supporting the BYOD or CYOD strategy.

The conclusions drawn from research results and data analysis, as well as the related findings and recommendations for future research (associated with this research) are discussed later in this chapter.

The previous chapters provided the following information:

Chapter One offered the introduction, background and scope of the research, as well as a broad overview of the entire research study.

Chapter Two reviewed existing literature of previous research in the area on the topic of this study, to facilitate an understanding and provide context relating to the focus of the research performed.

Chapter Three explained the methodology and design followed in this study.

Chapter Four discussed the data analysis and results of this study.

The layout of Chapter Five is illustrated in Figure 5.1 below.

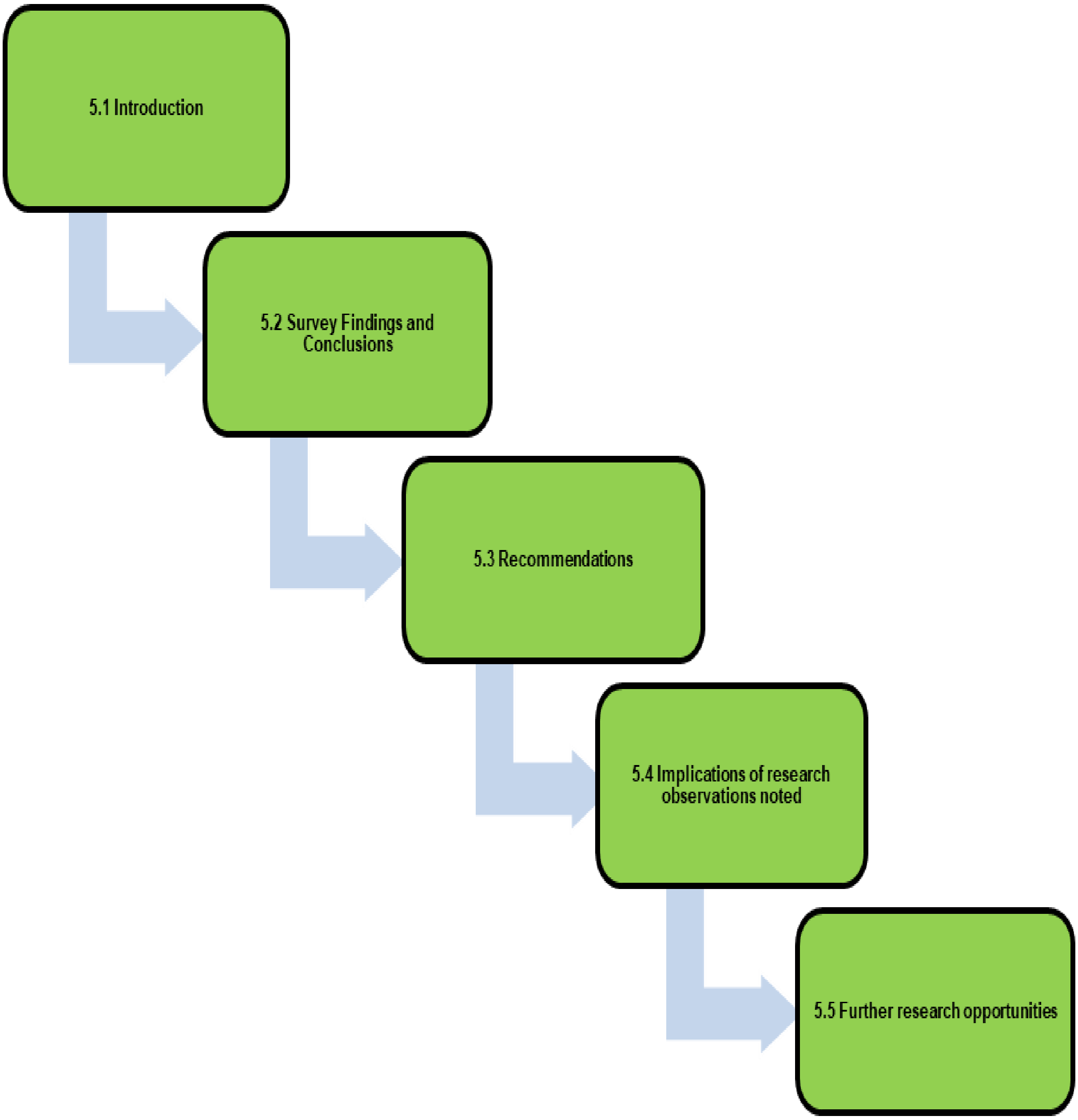

5.1 Introduction
5.2 Survey Findings and Conclusions
5.3 Recommendations
5.4 Implications of research observations noted
5.5 Further research opportunities

Figure 5.1: Layout of Chapter Five

5.2 Survey findings and conclusions

5.2.1 Objectives

The main objective of this research assignment was to ascertain if the connection of mobile devices in local government entities, located in the Namakwa District of the

Northern Cape, enhance efficiency and productivity, whilst the organisation ensures that the related risks are managed within its appetite of risk exposure.

With reference to Chapter Two, the associated risks pertaining to the use of mobile devices (user privacy risks, physical security risks, organisational and user information security risks and compliance risks) were discussed in this chapter.

The mitigation at an operational level associated with these risks, included in this study (supporting a specific technological solution, managing access requests, developing a security policy and/or procedure, providing user training and monitoring and maintenance of records relating to users with mobile device access) were also discussed in Chapter Two.

Furthermore, the abovementioned research question was supported by the literature reviewed in Chapter Two.

The following emanates from the results pertaining to the main research question:

- The use of mobile devices is important to the employees and management of these entities and enhances efficiency and productivity; and
- The risk management practices in these entities require improvement, more specifically relating to the following mitigation at an operational level:
    - Improvement or establishment of risk management functions in these entities;
    - Improvement in the risk management systems utilised with these entities;
    - Improvement of employee training and awareness;
    - Establishment, improvement or amendments to the Privacy and Security policy, Training and Awareness Procedure as well the Risk Management Policy;
    - Improvement of the control(s) pertaining to the record-keeping of information regarding users with mobile device access; and
    - Improvement relating to the re-evaluation process (on a periodic basis) pertaining to the mobile device users, ensuring that only valid and authorised users with proven requirements have access with these devices.

The findings are supported by the following:

A) Importance of mobile devices – impact on employee efficiency and productivity

- ***The majority of respondents confirm the importance of access with their mobile devices to the organisational network.***

Interpretation

Results from Chapter Four show that 37.50% of respondents indicated that access with mobile devices is very important, 27.08% indicated that access with mobile devices is important, 16.67% of respondents indicated that access with mobile devices is not so important, whilst 18.75% indicated it was not important at all.

- ***The majority of respondents confirm the importance of mobile devices according to their management in the achievement of organisational objectives.***

Interpretation

According to the results in Chapter Four, management in their organisations deem access with mobile devices as very important (39.58%), 41.67% of respondents indicated that their management deem it as important. However, 10.42% of respondents indicated that their management deem access with mobile devices as not so important, whilst 8.33% indicated that their management deem it as not important at all.

- ***Senior, middle and non-management personnel spent in excess of half of their work day on average (between 5.88 hours and 6.54 hours) on mobile devices.***

Interpretation

Results obtained from Chapter Four inform that the average time spent daily using mobile devices in these entities is as follows:

- Respondents in the senior management category indicated that they spent on average 5.88 hours daily using mobile devices;
- Respondents in the middle management category indicated that they spent on average 6.00 hours daily using mobile devices; and
- Respondents in the non-management category indicated that they spent on average 6.54 hours daily using mobile devices.

- ***A substantial number of respondents are in agreement that the use of mobile devices enhances their efficiency and productivity.***

Interpretation

Based on results in Chapter Four, the following was found:

- 52.50% of respondents strongly agree that the use of mobile devices enhances efficiency and productivity;
- 37.50% of respondents agree;
- 7.50% of respondents disagree; and
- 2.50% of respondents strongly disagree.

B) Mobile device-related risks

- ***Limited respondents confirms the occurrence of a security breach in organisational information pertaining to the use of mobile devices.***

  Interpretation

  According to the results detailed in Chapter Four, it was noted that around 10% of respondents indicated that their organisations have experienced a breach in terms of information security since permitting connections with mobile devices, 40.82% indicated that their organisations have not experienced any information security breach, while 48.98% of respondents indicated that they are not sure whether their organisations have experienced an information security breach.

C) Risk management practices

- ***The majority of respondents confirm that their entities have a risk management system in place.***

  Interpretation

  Results from Chapter Four reveal that a significant number of participants (67.34%) confirmed that their organisation does have a risk management system, whilst 18.37% indicated their organisation does not have a risk management system. The remainder of 14.29% indicated that they are not sure whether their organisation has a risk management system.

- ***Limited respondents confirm the existence of an electronic risk management system in their entities.***

  Interpretation

  Based on the results in Chapter Four, 22.86% of participants indicated that their organisation does have an electronic risk management system, 51.43% indicated that their organisation does not have such a system, while the rest of participants were not sure.

- ***Less than half of respondents confirm the existence of a risk management function in their entities.***

  Interpretation

  Results in Chapter Four inform that in 40.82% of participants indicated that their organisation does have a risk management function, 22.45% indicated that their organisation does not have such a function, while 36.73% of respondents indicated that they are not sure whether their organisation has a risk management function.

- ***In-house risk management functions in their organisations were confirmed by half of respondents.***

  Interpretation

  Based on results in Chapter Four, the following was noted:

  - 53.33% of participants confirmed that their organisations have an in-house risk management function;
  - 6.67% confirmed a co-sourced risk management function;
  - 6.67% confirmed having an outsourced risk management function; and
  - 33.33% of respondents indicated that they are not sure which type of risk management function their organisation has.

- ***Limited respondents are certain that a process exists pertaining to the approval of mobile device connections.***

  Interpretation

  Results in Chapter Four show that only 34% of respondents are certain that their organisation has a formal process in place on the approval of access requests pertaining to the use of mobile devices, 30% indicated that their organisation does not have such a process, while the rest of participants were not sure.

- ***Limited respondents confirm the existence of a policy or procedure as a guidance document pertaining to the use of mobile devices.***

  Interpretation

  Based on the results in Chapter Four, it was noted that only 30% of participants are certain that their organisation has formal policies and/or procedures in place pertaining to mobile devices, 36% believe their organisation does not have formal policies and/or procedures in place, while the rest of participants were not sure.

- ***A significant number of respondents confirm that no training is provided in instances where mobile devices are used.***

  Interpretation

  Results from Chapter Four show that training is provided on mobile devices in only 12% of organisations, whilst a significant number of respondents (70%)

confirmed that formal training is not provided. The remaining respondents were not sure.

- ***Limited respondents are certain that formal records are maintained for all employees with access to organisational networks with mobile devices.***

  Interpretation

  Results in Chapter Four indicate that 32% of respondents confirmed that formal records were maintained in their organisations pertaining to the use of mobile devices, 30% indicated that such records were not maintained, while 38% indicated that they were not sure whether their organisation maintained formal records.

- ***In 40% of instances, respondents are certain that their organisations re-evaluate approved mobile device access on a periodic basis (monthly, quarterly, twice a year or annually).***

  Interpretation

  Based on results in Chapter Four, the following was noted relating to the evaluation of mobile device accesses:

  - 20% of participants confirmed that their organisations assess the relevance of mobile device access on a monthly basis;
  - 15% confirmed the assessment happens on a quarterly basis;
  - 5% confirmed the assessment happens twice a year; and
  - 60% of respondents confirmed that they are not sure.

- ***A significant number of respondents is certain that their organisations update their risk registers on a periodic basis (monthly, quarterly, twice a year or annually).***

  Interpretation

  Based on results noted in Chapter Four, the following was noted relating to the updating of risk registers:

  - 6.12% of participants confirmed that their organisations update risk registers on a monthly basis;
  - 51.02% confirmed that it is done on a quarterly basis;
  - 2.04% confirmed that it is done twice a year;
  - 12.24% confirmed that it is done on an annual basis; and
  - 28.57% were not sure.

- ***The majority of respondents confirm that their entities have a risk management committee where risk reports are discussed.***

  Interpretation

  According to the results detailed in Chapter Four, it was noted that respondents in 64% of instances indicated that their organisation does have a risk management committee, 22% indicated that their organisation does not have such a committee and 14% were not sure whether their organisation has a risk management committee.

- ***More than half of the respondents confirm that their entity's risk management committee meets periodically (monthly, quarterly, twice a year or annually) to discuss risks relevant to the business.***

  Interpretation

  According to the results detailed in Chapter Four, it was noted that:

  - 4.88% (2 out of 41) of respondents indicated that their organisation's risk management committee meets on a monthly basis to discuss risks;
  - 60.98% (25 out of 41) confirmed that their risk management committee meets on a quarterly basis;
  - 4.88% (2 out of 41) confirms that it is an annual occurrence; and
  - 29.27% (12 out of 41) were not sure.

D) Effectiveness of risk management

- ***Limited respondents are certain that their organisation's risk relating to mobile devices is managed.***

  Interpretation

  Based on results noted in Chapter Four, 16.67% of respondents indicated that management of risks relating to mobile devices connected to their enterprise's network is very good, 19.94% confirmed it is good, whilst 27.78% of respondents indicated fairly good management of risks relating to mobile devices connected to their enterprise's network. However, 36.11% believed that these risks are poorly managed.

- ***The majority of respondents agrees that their entities' practice effective risk management.***

Interpretation

According to the results detailed in Chapter Four, the majority of participants (60.98%) agree that the risk management in their organisation is effective, whilst 9.76% strongly agree. However, 26.83% of respondents disagree that the risk management in their organisation is effective, whilst 2.44% strongly disagree.

5.2.2 Research objectives revisited

The research objectives as stated in Chapter One are:

1) To understand the importance of mobility to management and employees of local government entities in the Namakwa District of the Northern Cape, in achievement of organisational objectives; and
2) To understand the effectiveness of risk management where mobile device connections to local government networks are permitted in the Namakwa District of the Northern Cape.

5.2.2.1 Descriptive results: Research objective 1

The results of the analysis performed are utilised in answering the first research objective. The objective is to understand the importance of mobility to management and employees of local government entities in the Namakwa District of the Northern Cape, in achievement of organisational objectives. The research questions utilised in response to this research objective is as follows:

- Does management of local government entities in the Namakwa District of the Northern Cape deem mobility of employees as important to achieve organisational objectives.
- Do employees of local government entities in the Namakwa District of the Northern Cape deem connections with mobile devices to the entity's computer network(s) necessary to deliver on organisational objectives.

The conclusions drawn and the results pertaining to these research questions are discussed in Section 4.4.3.

5.2.2.2 Descriptive results: Research objective 2

The results pertaining to the analysis performed are utilised in answering the second research objective. The objective is to understand the effectiveness of risk management where mobile device connections to local government networks are permitted in the Namakwa District of the Northern Cape. The research questions utilised in response to this research objective are:

- Does the risk exposure increase in instances where mobile device connections to the local government entities in the Namakwa District is permitted;
- Is risk management effectively performed in instances where mobile device connections to the network of local government entities in the Namakwa District are allowed.

The conclusions drawn as well as the results pertaining to these research questions are discussed in Section 4.4.3.

Based on the previous discussions, it is evident that:

- Employees and management of local government entities in the Namakwa District consider the use of mobile devices as important and necessary in achievement of organisational objectives; and
- The risk management practices in these entities, specifically mitigation at an operational level, require improvement.

5.2.2.3 Conclusion

Based on the results previously presented, Table 5.1 summarises the conclusions to the research objectives.

Table 5.1: Research objectives revisited: Conclusions

Research objective	Conclusion
To understand the importance of mobility to management and employees of local government entities in the Namakwa District of the Northern Cape, in achievement of organisational objectives.	The majority of management as well as employees confirm that the use of mobile devices are important in the achievement of the organisational objectives.
To understand the effectiveness of risk management where mobile device connections to local government networks are permitted in the Namakwa District of the Northern Cape.	The risk management practices in these entities, specifically mitigation at an operational level, require improvement.

5.3 Recommendations

The main recommendations of the research are presented below.

5.3.1 Risk management function

It was found that just over 40% of respondents working in the local government entities in the Namakwa District of the Northern Cape are certain that their entities have a risk management function.

Recommendation

Based on the research results noted above, the following recommendations should be considered:

- Management must invest more time and resources to establish a risk management function if there is no such function in the enterprise;
- Where resources are a constraint in the establishment of such a function, it should be either co-sourced or outsourced;
- Transfer of skills to permanent personnel in a co-sourced or outsourced strategy should be a requirement in such consultancy agreements;
- The risk management policy should be revised to account for amendments if required; and
- Employees in the enterprise should be educated on risk management, and awareness created on a periodic basis.

5.3.2 Risk management system

It was found that although the majority of respondents working in the local government entities in the Namakwa District of the Northern Cape confirm that their organisations do have a risk management system, only 22.86% are certain that it is an electronic risk management system.

Recommendation

Based on the research results noted above, the following recommendations should be considered:

- Management should consider investing resources to implement an electronic risk management system which will allow for analysis of a specific risk as well as a cluster of risks, which will enhance risk management practices;
- Employees in the enterprise should be educated on the electronic risk management system; and
- Benefits associated with an electronic risk management system include the following items:
  - Risk reports are available immediately for all stakeholders having access to the system for continuous monitoring;

- Opportunity of viewing the top priority risks at any given time at different levels (strategic, divisional), and
- Inherent risk exposure as well as residual risk exposure of any specific risks is available at any given time.

5.3.3 Privacy and security policy/procedure

It was found that a limited number of respondents (30%) working in local government entities in the Namakwa District of the Northern Cape are certain that their organisations do have a policy and/or procedure document in place providing guidance to employees pertaining to mobile devices.

Recommendation

Based on the research results noted above, the following recommendation should be considered:

- Management must compile a privacy and security policy or procedure document pertaining to the use of mobile devices, approved by the relevant officials and committees, which provide guidance to employees.

5.3.4 Training and awareness

It was found that a substantial number of participants (70%) working in local government entities in the Namakwa District of the Northern Cape confirm that no training is provided in instances where mobile devices are used.

Recommendation

Based on the research results noted above, the following recommendations should be considered:

- Management must devote more time and/or resources to provide employees with the necessary training (periodically), creating security awareness of the associated risks pertaining to the use of mobile devices; and
- Training and awareness procedures should be amended where necessary.

5.3.5 Maintenance of formal mobile device users' records

It was found that limited respondents (32%) working in local government entities in the Namakwa District of the Northern Cape, are certain that their organisations maintain formal records of employees with access with mobile devices, whilst 40% of respondents confirmed that their organisations re-evaluate such access on a periodic basis (monthly, quarterly, twice a year or annually). However, 60% of respondents indicated that they are not sure if the re-evaluation process exists within their entities.

Recommendation

Based on the research results noted above, the following recommendations should be considered:

- Management must improve the controls pertaining to the recordkeeping of information regarding users with mobile device access and improve the re-evaluation process (on a periodic basis) pertaining to mobile devices, ensuring that only valid/authorised users are permitted;
- Benefits associated with the maintenance of formal records pertaining to users with mobile device access include the following:
    - Organisation is aware of which users have mobile device access to the network, including information such as the type of access and user information; and
    - In performing recordkeeping, other mitigation such as subsequent assessments could be easily performed, to ascertain whether the user still needs the access initially granted or taking away access of users considered to be more risky now than the when the original assessment was conducted.

5.4 Implications of research findings

Based on the research findings:

- Policies and procedure will require crafting or amendments prior to approval by the relevant officials and committees within the local government entities in the Namakwa District of the Northern Cape; and
- Training and Awareness to be improved with regards to Risk Management.

The implications of the research findings on policies and / or procedures is summarised below:

Table 5.2: Implications of Research Findings

Finding	Policy and/or Procedure	Explanation
Less than half of participants indicated that their organisation does have a risk management function.	Risk Management Policy; and Training and Awareness Procedure	Organisations not having a risk management function is in non-compliance with the Risk Management Policy; Employees in these entities to be trained with regards to Risk Management; and Frequency of employee training to be established

		and included in the Training and Awareness Procedure.
Limited respondents confirm the existence of an electronic risk management system in their entities	Risk Management Policy	Risk management processes not efficient.
Limited respondents confirm the existence of a policy or procedure as a guidance document pertaining to the use of mobile devices.	Privacy and Security Policy; and Training and Awareness Procedure	Employees not being aware of the process to follow in the event of a lost or stolen mobile device due the non-existence of a Privay and Security Policy / Procedure document; Employees in these entities to be trained with regards to the process to follow in the event of a lost or stolen mobile device; and Frequency of employee training to be established and included in the Training and Awareness Procedure.
A significant number of respondents confirm that no training is provided in instances where mobile devices are used.	Training and Awareness Procedure	Employees in these entities to be trained with regards to the process to follow in the event of a lost or stolen mobile device; and Frequency of employee training to be established and included in the Training and Awareness Procedure.
Limited respondents are certain that formal records are maintained for all employees with access to organisational networks with mobile devices; and In 40% of instances, respondents are certain that their organisations re-evaluate approved mobile device access on a periodic basis	Privacy and Security Policy	Organisation not having a complete list of users with mobile device access as well as the type of access.

5.5 Further research opportunities

There were limitations relating to this study. The limiting factors experienced relate to not receiving a written consent letter from the leadership of all entities within the scope of the study, granting the researcher permission to approach employees within their entities during the data collection phase; participant's daily tasks (at work) taking preference, resulting in a slow response rate relating to the completion and return of Research Questionnaire documents; and the fact that this study exclusively focused on the municipalities in the Namakwa District of South Africa.

Another limitation is the fact that the research focused more on the existence and/or effectiveness of mitigation relating to the operational level whilst utilising mobile devices in local government entities in the Namakwa District of the Northern Cape.

Research relating to the strategic level mitigation within organisations was previously performed. However, further research opportunities that exist (and could be undertaken) which were not included in this study, although identified during the empirical study, relate to:

- Improvement of internal controls (use of matrixes) governing the risks linked to the utilisation of mobile devices;
- Worthiness and cost pertaining to the use of mobile devices by organisations;
- Verification of other security solutions linked to mobile device use; and
- Development of a methodology relating to risk assessment whilst using mobile devices, to prioritise the treatment of higher risk exposure prior to spending time on the remaining risks.

REFERENCES

Adedolapo, A. 2016. Bring your own device (BYOD) adoption in South African SMEs. https://open.uct.ac.za/bitstream/.../thesis_com_2016_akin_adetoro_adedolapo.pdf [10 March 2019].

Afreen, K. 2014. Bring your own device (BYOD) in higher education: Opportunities and challenges. http://scholar.google.co.za/scholar?start=10&q=byod&hl=en&as_sdt=0,5&rlz=1Y1XIUG_enZA513ZA513 [20 April 2017].

Akram, R., Markantonakis, K. & Holloway, R. 2016. Challenges of security and trust of mobile devices as digital avionics components. https://arxiv.org/pdf/1605.00446.pdf [09 October 2018].

Allen, R. 1990. *The Concise Oxford Dictionary*. https://archive.org/details/conciseoxforddic00alle [09 October 2018].

Ames, B., Brown, F., Bogert, J., Creer, M., Lourens, J., Patel, R., Rai, S. & Stein, S. 2016. *An internal auditor's guide to understanding and auditing smart devices.* https://na.theiia.org/standards-guidance/Member%20Documents/GTAG-Auditing-Smart-Devices.pdf [09 May 2017].

Aven, T. 2015. *Risk assessment and risk management: Review of recent advances on their foundation*. https://ac.els-cdn.com/S0377221715011479/1-s2.0-S0377221715011479-main.pdf?_tid=748a9904-6c3a-42f5-9383-d637f7ee4b35&acdnat=1524181679_606e459901e201a8b8101cfd6969a50a [20 April 2018].

Bais, A. 2016. *Security risks associated with BYOD*. https://projekter.aau.dk/projekter/files/244720006/BYOD_Security_AhmadBais.pdf [06 March 2019].

Banerjee, A. & Wallace, S. 2014. *The pillars of a next-generation enterprise mobility solution.* https://www.symantec.com/content/en/us/enterprise/white_papers/b-hr-symantec-enterprise-mobility-wp.en-us.pdf [09 March 2017].

Bann, L., Singh, M. & Samsudin, A. 2015. *Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment*. http://www.sciencedirect.com/science/article/pii/S1877050915035747 [8 March 2017]

Beech, J. 2015. *Doing your business research project.* London: SAGE.

Bhat, A. 2019. *Sample: Definition, methods, types with examples*. https://www.questionpro.com [18 July 2019].

Bourne, A., Donatti, C., Holness, S. & Midgley, G. 2012. *Climate change. Vulnerability assessment for the Namakwa District Municipality.* https://www.weadapt.org/sites/weadapt.org/files/legacy-new/knowledge-base/files/51c4c23ad02f8final-vulnerability-assessment-full-technical-report-ndm-with-cover.pdf [12 May 2019].

Brand, J. 2013. *The governance of significant enterprise mobility security risks.* https://scholar.sun.ac.za/bitstream/handle/10019.../brand_governance_2013.pdf? [17 September 2017].

Brodin, M. 2016. *Mobile device strategy: A management framework for securing company information*. www.diva-portal.org/smash/record.jsf?pid=diva2:1048747 [10 March 2019].

Bruwer, J. & Siwangaza, L. 2016. *Is the Control Environment a Basis for Customised Risk Management Initiatives in South African Small, Medium and Micro Enterprises?* http://www.zbw.eu/econis-archiv/bitstream/handle/11159/1376/1006130519.pdf?sequence=1 [10 May 2020].

Callegaro, M., Manfreda, K. & Vehovar, V. 2015. *Web survey methodology*. Los Angeles, CA: SAGE. https://uk.sagepub.com/sites/default/files/upm-binaries/68628_Callegaro%2C_Web_Survey_Methodolgy_Chapter_6.pdf [09 October 2018].

Cardinal, D. 2016. *How the smartphone changed everything, or, the rise of BYOD in the workplace*. https://arstechnica.com/information-technology/2016/01/how-the-smartphone-changed-everything-or-the-rise-of-byod-in-the-workplace/ [7 March 2017].

Chapman, C. & Ward, S. 2003. *Project risk management: Processes, techniques and insights*. http://index-of.co.uk/Project%20Management/John%20 John Wiley & Sons%20&%20Sons%20-%20Project%20Risk%20Management%20-%20Processes_%20Techniques%20&%20Insights.pdf [13 February 2018].

Chen, H. & Li, W. 2017. *Mobile device users' privacy security assurance behaviour: A* technology threat avoidance perspective. https://www-emeraldinsight-com.libproxy.cput.ac.za/doi/full/10.1108/ICS-04-2016-0027 [14 February 2019].

Cherry, K. 2019. *History and key concepts of behavioural psychology*. https://www.verywellmind.com/behavioral-psychology-4157183 [21 June 2019].

Christoffersen, P. 2012. *Elements of financial risk management.* New York: Elsevier. http://fanarco.net/books/risk/Elements.of.Financial.Risk.Management.pdf [12 March 2018].

Collis, J. & Hussey, R. 2014. *Business research: A practical guide for undergraduate & postgraduate students.* Basingstoke, UK: Palgrave Macmillan.

Creswell, R. 2008. *The use of theory – description.* http://jdst.sagepud.com/file/upm-binaries/22781_Chapter3.pdf [21 June 2019].

UCLA. n.d. *What does Cronbach's alpha mean?* https://stats.idre.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/ [17 May 2019].

De Shield, L. 2017. *The challenges of implementing Bring Your Own Device*. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=5894&context [10 March 2019].

Dhingra, M. 2016*. Legal issues in secure implementation of Bring Your Own Device (BYOD).* http://www.sciencedirect.com/science/article/pii/S1877050916000326 [08 March 2017].

Disterer, G. & Kleiner, C. 2013. *BYOD Bring Your Own Device.* http://www.sciencedirect.com/science/article/pii/S221201731300159X [08 March 2017].

Dubihlela, J. & Nqala. L. 2017. Internal control systems and the risk performance characterizing small and medium manufacturing firms in the Cape Metropole. International journal of business and management studies, 9(2) pp. 87-103.

Eslahi, M., Naseri, M., Hashim, H., Tahir, N. & Saad, E. 2013. BYOD: *Current state and security challenges.* https://s3.amazonaws.com/academia.edu.documents/34233704/BYOD-Current_State_and_Security_Challenges.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1539086782&Signature=kj5ywYiCHCPJDyIIxnFLkVz00RU%3D&response-content-disposition=inline%3B%20filename%3DBYOD-Current_State_and_Security_Challeng.pdf [09 October 2018].

Evans, D. 2013. *What is BYOD and why is it important.*

https://www.ware247.co.uk/Content/CMS/Files/What%20is%20BYOD.pdf [11 March 2017].
Flick, U. 2015. *Introducing research methodology*. 2nd ed. Berlin: Freie Universtität.

Farnsworth, B. 2019. *Qualitative vs quantitative research – what is what?* https://imotions.com/blog/qualitative-vs-quantitative-research [12 July 2019].

Fraser, J. & Simkins, B. (eds.). 2010. *Enterprise risk management: Today's leading research and best practices for tomorrow's executives.* Hoboken, NJ: John Wiley & Sons.

https://epdf.pub/enterprise-risk-management-todays-leading-research-and-best-practices-for-tomorr.html [24 August 2018].

Bellamy, F.D. 2014. *Enterprises without strong BYOD policies risk major data breach*. https://search-proquest-com.libproxy.cput.ac.za/docview/1560542000/fulltext/E455E12D663A4CDEPQ/1?accountid=26862 [14 February 2019].

Gaff, B. 2015. *BYOD? OMG!* https://cput.primo.exlibrisgroup.com/discovery/fulldisplay?docid=gale_ofa425615088&context=PC&vid=27CPUT_INST:CPUT&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central [14 February 2019].

Garba, A., Armarego, J. & Murray, D. 2015. *A policy-based framework for managing information security and privacy risks in BYOD environment.* http://www.ijettcs.org/Volume4Issue2/IJETTCS-2015-04-23-122.pdf [11 March 2017].

Gliem, J. & Gliem, R. 2003. *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*. https://scholarworks.iupui.edu/bitstream/handle/1805/344/Gliem+&+Gliem.pdf?sequence=1 [22 July 2019].

Goertzen, M. 2017. *Introduction to quantitative research and data*. https://journals.ala.org/index/php/ltr/article/view/6325/8275 [12 July 2019].

Gomez, R. 2013. *Security solutions in consumer goods & retail.* https://www.ie.edu/fundacion_ie/Home/Documentos/Information_Security_in_Retail_&_CG_-_IE_Foundation_and_Ernst_&_Young_2.pdf [14 May 2018].

Greenfield, T. & Greener, S. (eds.). 2016. *Research methods for postgraduates.* 3rd ed. New York: John Wiley & Sons.

Gregoriou, G. (ed.). 2007. *Advances in risk management*. Basingstoke, UK: Palgrave Macmillan. ISBN13 9780230019164.

Gustav, A. & Kabanda, S. 2016. *BYOD adoption concerns in the South African financial institution sector.*

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1017&context=confirm2016 [08 May 2020].

Hanlin, C., Jiao, L., Thomas, H. & Xiaowei, L. 2013. *Security challenges of BYOD: A security education, training and awareness perspective*. https://minerva-access.unimelb.edu.au/handle/11343/33347 [11 March 2017]

Harris, M., Patten, K. & Regan, E. 2013. *The need for BYOD mobile device security awareness and training*. http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/14/ [11 March 2017].

Heijblom, R. 2015. *Controlling risks when integrating mobility and enterprise resource planning (ERP*). https://dspace.library.uu.nl/.../1874/.../Master%20thesis%20Rodi%20Heijblom.pdf? [10 March 2019].

Hemdi, M. & Deters, R. 2016. *Data management in mobile enterprise applications.* https://ac.els-cdn.com/S1877050916318142/1-s2.0-S1877050916318142-main.pdf?_tid=4966f911-9300-484f-a944-c54a460ba8ee&acdnat=1526258158_a23abf63de70c236af502b78c59a21ef [14 May 2018].

Hetting, C. 2014. *Mitigating security & compliance risks with EMM.* https://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Heavy_Reading-Mitigating_Security_and_Compliance_Risks_with_EMM.pdf [14 May 2018].

Hinkes, A. 2014. *BYOD policies: A litigation perspective.* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2014_sac/2014_sac/byod_policies.pdf [11 March 2017].

Hopkin, P. 2010. *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management.* Philadelphia, PA: Kogan Page. http://www.hostgator.co.in/files/writeable/uploads/hostgator12628/file/fundamentalsofriskmanagement.pdf [30 May 2018].

Horcher, K. 2005. *Essentials of financial risk management.* Hoboken, NJ: John Wiley & Sons. https://pdfs.semanticscholar.org/1471/8151be2ded6a8341e5c8964abc8f515319b9.pdf?_ga=2.210461653.1587717689.1579763116-1037942919.1578822642 [3 April 2019].

Hornby, A. 2010. *Oxford Advanced Learner's Dictionary.* 8th ed. Oxford, UK: Oxford University Press.

Hull, J. 2015. *Risk management and financial institutions*. 4th ed. Hoboken, NJ: John Wiley & Sons. http://www.simonfoucher.com/MBA/FINA%20695%20-%20Risk%20Management/riskmanagementandfinancialinstitutions4theditionjohnhull-150518225205-lva1-app6892.pdf [25 June 2018].

Jamaluddin, H., Ahmad, Z., Alias, M. & Simun, M. 2015. *Personal Internet use: The use of personal mobile devices at the workplac*e. www.sciencedirect.com/science/article/pii/S1877042815004280 [20 April 2017].

Jansen van Vuuren, L., Reyers, M. & Van Schalkwyk, C. 2017. *Assessing the impact of Solvency Assessment and Management on risk management in South African insurance companies*. https://www.ajol.info/index.php/sabr/article/view/155434 [10 May 2020].

Kelley, R. n.d. *Ethics and technology: Cell phones*. https://ethicsandtechnology.weebly.com/cell-phones.html [18 February 2019].

Kenton, W. 2019. *Population definition*. https://www.investopedia.com/terms/p/population.asp [15 July 2019].

Khan, J., Abbas, H. & Al-Muhtadi, J. 2015. *Survey of mobile user's data privacy threats and defence mechanisms*. http://www.sciencedirect.com/science/article/pii/S1877050915017044 [20 April 2018].

Kielbus, A. & Karpisz, D. 2019. *Risk Management as a process security tool.* https://content.sciendo.com/view/journals/czoto/1/1/article-p234.xml [08 May 2020].

Kim, D. 2018. *Cell phone use at work: Where's the line?* https://www.workplaceethicsadvice.com/2018/11/cell-phone-use-at-work-wheres-the-line.html [18 February 2019].

Kim, T., Shulman, K., Hersh, W., Keister, H. 2012. *IIA International standards for the professional practice of internal auditing*. https://dl.theiia.org/ACGAPublic/International-Standards-and-Government-Audit-Standards-(GAGAS)-Comparison-2nd-Edition.pdf [23 June 2018].

Kleiner, C. & Disterer, G. 2015. *Ensuring mobile device security and compliance at the workplace*. http://www.sciencedirect.com/science/article/pii/S1877050915026253 [11 March 2017].

Larson, M. & Weil, M. 2013. *Mobile device discovery and investigations: Getting smart about smartphones*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-fas-mobile-device-discovery-and-investigations-08162013.pdf [14 May 2018].

Lima, A., Sousa, B., Cruz, T. & Simoes, P. n.d. *Security for mobile device assets: A survey*. https://www.researchgate.net/profile/Tiago_Cruz3/publication/312070802_Security_monitoring_for_mobile_device_assets_a_survey/links/592f4fffa6fdcc89e781ed09/Security-monitoring-for-mobile-device-assets-a-survey.pdf [09 October 2018].

Loose, M., Weeger, A. & Gewald, H. 2013. *BYOD – the next big thing in recruitment? Examining the determinants of BYOD service adoption behaviour from the perspective of future employees*. http://aisel.aisnet.org/amcis2013/EndUserIS/GeneralPresentations/12/ [11 March 2017].

Ludwig, S. 2018. *Why organizations should still care about BYOD.* https://search-proquest-com.libproxy.cput.ac.za/docview/2052775065?rfr_id=info%3Axri%2Fsid%3Aprimo [14 February 2019].

Lydon, E. 2014. *The benefits and threats of BYOD in a SME enterprise*. www.diva-portal.org/smash/record.jsf?pid=diva2:1022207 [06 March 2019].

Maggie, P. 2015. *Tablets shake up the trading floor.* https://search-proquest-com.libproxy.cput.ac.za/docview/1748608624?rfr_id=info%3Axri%2Fsid%3Aprimo [14 February 2019].

McDonnell, C., Fox, J., Moroney, M. & Wills, S. 2014. *Mobile devices: Secure or security risk?* https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/mobile_device_secure_security_risk.pdf [14 May 2018].

McIntosh, C. 2015. *Cambridge advanced learner's dictionary.* Cape Town: Cambridge University Press. ISBN 978-1-107-65313-9.

Miakotko, L. n.d. *The impact of smartphones and mobile devices on human health and life.* https://www.nyu.edu/classes/keefer/waoe/miakotkol.pdf [28 February 2019].

Miller, K., Voas, J. & Hurlburt, G. 2012. *BYOD: Security and privacy considerations*. https://s3.amazonaws.com/academia.edu.documents/30666416/MVH2012.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1539086547&Signature=CXK%2FJ%2ByQFa

sQQijttefDhISuJ2A%3D&response-content-disposition=inline%3B%20filename%3DBYOD_Security_and_Privacy_Considerations.pdf [09 October 2018].

Moeller, R. 2009. *Brink's modern internal auditing: A common body of knowledge.* 7th ed. Hoboken, NJ: John Wiley & Sons. https://mstakimch.files.wordpress.com/2012/09/brink_s-modern-internal-auditing-7th-edition.pdf [22 September 2018].

Mowafi, Y., Abou-Tair, D., Zmily, A., Al-Aqarbeh, T. Abilov, M. & Dmitriyevr, V. 2015. *Exploring a context-based network access control for mobile devices.* http://www.sciencedirect.com/science/article/pii/S1877050915026654 [20 April 2017].

Municipalities of South Africa. 2020. *Municipalities.* https://municipalities.co.za/ [24 January 2020].

Musarurwa, A. & Flowerday, S. 2018. *The BYOD Information Security Challenge for CIOs*. https://scholar.google.co.za/scholar?hl=en&as_sdt=0%2C5&q=The+BYOD+Information+Security+Challenge+for+CIOs&btnG= [08 May 2020].

Musarurwa, A. & Flowerday, S. 2019. *Information Privacy in the BYOD*. https://scholar.google.co.za/scholar?hl=en&as_sdt=0%2C5&q=Information+Privacy+in+the+BYOD%2C+Musarurwa&btnG= [08 May 2020].

Olsson, C. 2002. *Risk management in emerging markets*. New York: Pearson Education. http://www.fanarco.net/books/risk/Carl_Olsson_-_Risk_Management_In_Emerging_Markets_-_How_To_Survive_And_Prosper_[2002].pdf [18 May 2018].

Pereira, T., Barreto, L. & Amaral, A. 2017. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, 13:1253–1260. https://www.sciencedirect.com/science/article/pii/S2351978917306820/pdfft?md5=9d9658e8a0f2830d26a435b10261eaa6&pid=1-s2.0-S2351978917306820-main.pdf [12 September 2018].

Phillips, C. 2014. *Information security governance implementation within the mobile device environment*. https://open.uct.ac.za/bitstream/handle/.../thesis_com_2014_com_phillips_c.pdf? [06 March 2019].

Pillay, A., Diaki, H., Nham, E., Senanayake, S., Tan, G. & Deshpande, S. 2013. *Does BYOD increase risks or drive benefits?* https://minerva-access.unimelb.edu.au/handle/11343/33345 [11 March 2017].

Porro, A. 2014. *BYOD, COPE or CYOD? How to choose the right enterprise mobility strategy for your business.* https://www.itproportal.com/2014/08/25/byod-cope-or-cyod-how-to-choose-the-right-enterprise-mobility-strategy-for-your-business/ [28 February 2019].

Prathapan, K. 2014. *Research methodology for scientific research*. New Delhi: I K International. ISBN-13: 9789382332855.

Ragab, M. & Arisha, A. 2017. *Research methodology in business: A starter's guide.* https://www.sciedupress.com/journal/index.php/mos/article/download/12708/7848 [15 July 2019].

Remenyi, D. 2013. *Field methods for academic research: Interviews, focus groups & questionnaires*. Sonning Common, UK: Academic Conferences & Publishing Limited. ISBN: 978-1-908272-77-5.

Revenaugh, D & Schweigert, M. 2013. *BYOD: Moving toward a more mobile and productive workforce*. http://digitalcommons.mtech.edu/business_info_tech/3/ [11 March 2017].

Rowton, M. n.d. *Managing application security of mobile devices: Bring Your Own Device.* http://attackprevention.com/whitepapers/mobile_device_management.pdf [11 March 2017].

Ruxwana, N. & Msibi, M. 2018. *A South African university's readiness assessment for bringing your own device for teaching and learning.*

http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2018000100011

[08 May 2020].

Sahd, L. & Rudman, R. 2016. *Mobile technology risk management.* https://scholar.sun.ac.za/bitstream/handle/10019.1/99222/sahd_mobile_2016.pdf?sequence=1&isAllowed=y [14 May 2018].

Sahd, L. 2015. *A structured approach to the identification of the significant risks related to enterprise mobility solutions at a mobile technology component level*. https://scholar.sun.ac.za/bitstream/handle/10019.1/.../sahd_structured_2015.pdf? [17 September 2017].

Saunders, M., Lewis, P. & Thornhill, A. 2016. *Research methods for business students.* 7th ed. Upper Saddle River, NJ: Pearson Education. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.7307&rep=rep1&type=pdf [11 April 2018].

Schwartz, K. 2015. *Managing a mobile workforce*. https://search-proquest-com.libproxy.cput.ac.za/docview/1673377021?rfr_id=info%3Axri%2Fsid%3Aprimo [14 February 2019].

Sekaran, U. & Bougie, R. 2013. *Research methods for business*. 6th ed. New York: John Wiley & Sons.

Shacklett, M. 2016*. Mobile devices in the workplace: Three situations that could get awkward.* https://www.techrepublic.com/article/mobile-devices-in-the-workplace-three-situations-that-could-get-awkward/ [18 February 2019].

Sheldon, R. 2013a. *BYOD vs COPE: Why corporate device ownership could make a comeback*. https://searchmobilecomputing.techtarget.com/feature/BYOD-vs-COPE-Why-corporate-device-ownership-could-make-a-comeback [28 February 2019].

Sheldon, R. 2013b. *Wearable computing devices could have enterprise prospects.* http://searchmobilecomputing.techtarget.com/opinion/Wearable-computing-devices-could-have-enterprise-prospects [06 March 2017].

Shim, J., Mittleman, D., Welke, R., French, A. & Guo, J. 2013. *Bring Your Own Device (BYOD): Current status, issues, and future directions.* http://aisel.aisnet.org/amcis2013/Panels/PanelSubmissions/4/ [11 March 2017].

Siddiqui, R. 2014. *Bring Your Own Device (BYOD) in higher education: Opportunities and challenges*. http://scholar.google.co.za/scholar?start=10&q=byod&hl=en&as_sdt=0,5&rlz=1Y1XIUG_enZA513ZA513 [11 March 2017].

Siwangaza, L. & Dubihlela, J.2017. Internal Organisational Environments of SMMEs in Cape Town, and Effect on Preventative, Detective and Directive Internal Controls. SAAA National Teaching and Learning and Regional Conference Proceedings, 44-57. http:// www.saaa.org.za/Downloads [Accessed 5 April 2017]

Smith, W. 2014. *Pharos English Dictionary for South African schools.* Cape Town: NB Publishers.

Souppaya, M. & Scarfone, K. 2013. *Guidelines for managing the security of mobile devices in the enterprise*. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [07 March 2017].

South Africa. 2003. *Municipal Finance Management Act No. 56 of 2003.* http://www.ffc.co.za/legislation [27 March 2019].

South Africa. 1996. *The Constitution of the Republic of South Africa.*

South African Local Government Association (SALGA). n.d. *Risk Management Framework.* http://www.salga.org.za [27 March 2019].

Spencer Pickett, K.H. 2005a. *Auditing the risk management process*. Chichester, UK: John Wiley & Sons. https://pdfs.semanticscholar.org/467e/6e49bdbadfef0899da6f25514e4dea4c3890.pdf [12 July 2018].

Spencer Pickett, K.H. 2005b. *The essential handbook of internal auditing*. Chichester, UK: John Wiley & Sons.

Steinberg, R., Martens, F., Everson, M. & Nottingham, L. 2004. *Enterprise risk management – integrated framework*. http://www.macs.hw.ac.uk/~andrewc/erm2/reading/ERM%20-%20COSO%20Application%20Techniques.pdf [23 August 2018].

Stumpfegger, E. 2017. *Qualitative versus quantitative research*. https://www.munich-business-school.de/insights/en/2017/qualitative-vs-quantitative-research [12 July 2019].

Tairov, I. 2016. *Enterprise mobility – a solution for increased business efficiency*. https://dlib.uni-svishtov.bg/bitstream/handle/10610/3132/p587__BMBook3eng2016_78_88.pdf?sequence=1&isAllowed=y [09 October 2018].

Tiganoaia, B., Niculescu, A., Negoita, O. & Popescu, M. 2019. *A New Sustainable Model for Risk Management - RiMM.* https://www.mdpi.com/2071-1050/11/4/1178 [08 May 2020].

Tonmoy, F., Rissik, D. & Palutikof, J. 2019. *A three-tier risk assessment process for climate change adaption at a local scale.* https://link.springer.com/article/10.1007/s10584-019-02367-z [08 May 2020].

Treleaven, R. 2014. *Mobile device management: Three important questions your municipality needs to answer*. https://search-proquest-com.libproxy.cput.ac.za/docview/1686405577/fulltext/13B90884CDB54769PQ/1?accountid=26862 [14 February 2019].

Tsiga, Z., Emes, M. & Smith, A. 2017. *Implementation of a risk management simulation tool.* https://ac.els-cdn.com/S1877050917322214/1-s2.0-S1877050917322214-main.pdf?_tid=21e64b00-0213-41b9-8940-f83c19338b6a&acdnat=1520502988_8401318b2770bc13bd9bdb65fd1c41d2 [08 March 2017].

Tupa, J., Simota, J. & Frantisek, S. 2017. *Aspects of risk management implementation for Industry 4.0*. https://ac.els-cdn.com/S2351978917304560/1-s2.0-S2351978917304560-main.pdf?_tid=c2d51cbf-79c5-4a2d-9fd8-9d19e21e7c39&acdnat=1520502030_5a34bdccc0b94d581a184c203e512769 [08 March 2017].

Twinomurinzi, H. & Mawela, T. 2014. *Employee perceptions of BYOD in South Africa: Employers are turning a blind eye?* https://dl.acm.org/doi/abs/10.1145/2664591.2664607 [08 May 2020].

Valsamakis, A., du Toit & G. Vivian, R. 2010. *Risk management.* Upper Saddle River, NJ: Pearson Education

Valsamakis, A., Vivian, R. & Du Toit, G. 2005. *Risk management: Managing enterprise risks*. Sandton, South Africa: Heinneman.

Van der Poll, H. & Mthiyane, Z. 2018. *The interdependence of risk management, corporate governance and management accounting.*

https://www.ajol.info/index.php/sabr/article/view/178570 [10 May 2020].

Van Kessel, P., Layman, J., Blackmore, J., Burnet, I. & Harada, S. 2013. *Bring your own device: Security and risk considerations for your mobile device program.* http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf [07 March 2017].

Vasvari, T. 2015. *Risk, Risk Perception, Risk Management – a Review of the Literature.* https://www.researchgate.net/profile/Tamas_Vasvari/publication/278410839_Risk_Risk_Perception_Risk_Management/links/5580915408ae607ddc322683/Risk-Risk-Perception-Risk-Management.pdf [10 May 2020].

Vignesh, U. & Asha, S. 2015. *Modifying security policies towards BYOD*. http://www.sciencedirect.com/science/article/pii/S1877050915005244 [08 March 2017].

Walliman, N. 2011. *Research methods: The basics.* London: Taylor & Francis. ISBN13 9781138693999.

Weldon, D. 2014. *Choosing BYOD vs CYOD? The path to both is secure data.* https://search-proquest-com.libproxy.cput.ac.za/docview/1553263270?rfr_id=info%3Axri%2Fsid%3Aprimo [14 February 2019].

Wood, L. 2017. *Global enterprise application market 2019–2022.* https://cput.primo.exlibrisgroup.com/view/action/uresolver.do?operation=resolveService&package_service_id=1358217330004036&institutionId=4036&customerId=4035 [14 February 2019].

Wu, D., Olson, D. & Birge, J. (eds.). 2011. *Quantitative financial risk management.* New York: Springer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.9830&rep=rep1&type=pdf [15 June 2018].

Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Grob, T., Laing, C. & Van Moorsel, A. 2014. *Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging*. www.sciencedirect.com/science/article/pii/S2212017314003454 [20 April 2017].

Zimeng, H. 2015. *Security of mobile devices and wi-fi networks*. www.theseus.fi/handle/10024/94480 [06 March 2019].

APPENDIX A: FREQUENCY TABLE REPORT

26/08/2019 11:55:07

Frequency Table Report

Dataset ...\Patrick Otto - Captured RAW DATA for Research V4a.NCSS

Frequency Distribution of A01 Gender

A01 Gender	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Male	32	32	64.00%	64.00%	|||||||||||||||||||||||||
2 Female	18	50	36.00%	100.00%	||||||||||||||

Frequency Distribution of A02 AgeCat

A02 AgeCat	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 19 – 25	6	6	12.00%	12.00%	||||
2 26 – 35	17	23	34.00%	46.00%	|||||||||||||
3 36 – 45	18	41	36.00%	82.00%	||||||||||||||
4 46 – 55	8	49	16.00%	98.00%	||||||
5 56 – 65	1	50	2.00%	100.00%	|

Frequency Distribution of A03 Yrs_Exp

A03 Yrs_Exp	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	6				
0.1	2	2	4.55%	4.55%	|
0.8	1	3	2.27%	6.82%	|
1	3	6	6.82%	13.64%	||
3	2	8	4.55%	18.18%	|
4	1	9	2.27%	20.45%	|
5	3	12	6.82%	27.27%	||
6	2	14	4.55%	31.82%	|
8	1	15	2.27%	34.09%	|
9	3	18	6.82%	40.91%	||
10	3	21	6.82%	47.73%	||
11	3	24	6.82%	54.55%	||
12	2	26	4.55%	59.09%	|
14	2	28	4.55%	63.64%	|
15	2	30	4.55%	68.18%	|
16	1	31	2.27%	70.45%	|
18	1	32	2.27%	72.73%	|
19	2	34	4.55%	77.27%	|
20	4	38	9.09%	86.36%	|||
23	1	39	2.27%	88.64%	|
26	1	40	2.27%	90.91%	|
27	1	41	2.27%	93.18%	|
32	1	42	2.27%	95.45%	|
34	1	43	2.27%	97.73%	|
38	1	44	2.27%	100.00%	|

The number of missing values is 6.
The overall count including missing values is 50.
The overall percentage of missing values is 12.00%.

Frequency Distribution of A04 Nr_Emp

A04 Nr_Emp	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	11				
62	1	1	2.56%	2.56%	|
82	1	2	2.56%	5.13%	|
83	1	3	2.56%	7.69%	|
84	3	6	7.69%	15.38%	|||
85	1	7	2.56%	17.95%	|
87	1	8	2.56%	20.51%	|
90	3	11	7.69%	28.21%	|||
96	1	12	2.56%	30.77%	|
98	1	13	2.56%	33.33%	|
100	4	17	10.26%	43.59%	||||
103	3	20	7.69%	51.28%	|||
105	9	29	23.08%	74.36%	|||||||||
106	1	30	2.56%	76.92%	|
109	1	31	2.56%	79.49%	|
120	1	32	2.56%	82.05%	|
123	1	33	2.56%	84.62%	|
140	1	34	2.56%	87.18%	|
149	3	37	7.69%	94.87%	|||
164	1	38	2.56%	97.44%	|
174	1	39	2.56%	100.00%	|

The number of missing values is 11.
The overall count including missing values is 50.
The overall percentage of missing values is 22.00%.

Frequency Distribution of A05 Posit_Level

A05 Posit_Level	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Senior Management	9	9	18.00%	18.00%	|||||||
2 Middle Management	16	25	32.00%	50.00%	||||||||||||
3 Non Management	25	50	50.00%	100.00%	||||||||||||||||||||

Frequency Distribution of B06 Mob_use

B06 Mob_use	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Yes	42	42	84.00%	84.00%	
	|||||||||||||||||||||||||||||||||				
2 Not sure	3	45	6.00%	90.00%	||
3 No	5	50	10.00%	100.00%	||||

Frequency Distribution of B07 Mob_Types

B07 Mob_Types	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent

<table>
<tr><td>Missing</td><td>8</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Laptops</td><td>30</td><td>30</td><td>71.43%</td><td>71.43%</td><td>||||||||||||||||||||||||||||</td></tr>
<tr><td>3 Tablets</td><td>1</td><td>31</td><td>2.38%</td><td>73.81%</td><td>|</td></tr>
<tr><td>4 Other</td><td>1</td><td>32</td><td>2.38%</td><td>76.19%</td><td>|</td></tr>
<tr><td>1_2 Laptop_Smartphones</td><td>1</td><td>33</td><td>2.38%</td><td>78.57%</td><td>|</td></tr>
<tr><td>1_2_3 Laptop_Smartp_Tablet</td><td>5</td><td>38</td><td>11.90%</td><td>90.48%</td><td>||||</td></tr>
<tr><td>1_3 Laptop_Tablet</td><td>4</td><td>42</td><td>9.52%</td><td>100.00%</td><td>|||</td></tr>
</table>

The number of missing values is 8.
The overall count including missing values is 50.
The overall percentage of missing values is 16.00%.

Frequency Distribution of B08 Remot_ Acc_Org_Info

<table>
<tr><th>B08 Remot_ Acc_Org_Info</th><th>Count</th><th>Cumulative Count</th><th>Percent</th><th>Cumulative Percent</th><th>Graph of Percent</th></tr>
<tr><td>Missing</td><td>9</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Yes</td><td>24</td><td>24</td><td>58.54%</td><td>58.54%</td><td>|||||||||||||||||||||||</td></tr>
<tr><td>2 No</td><td>17</td><td>41</td><td>41.46%</td><td>100.00%</td><td>||||||||||||||||</td></tr>
</table>

The number of missing values is 9.
The overall count including missing values is 50.
The overall percentage of missing values is 18.00%.

Frequency Distribution of B09 Period_use_Mob

<table>
<tr><th>B09 Period_use_Mob</th><th>Count</th><th>Cumulative Count</th><th>Percent</th><th>Cumulative Percent</th><th>Graph of Percent</th></tr>
<tr><td>Missing</td><td>39</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4 Not used</td><td>2</td><td>2</td><td>18.18%</td><td>18.18%</td><td>|||||||</td></tr>
<tr><td>5</td><td>2</td><td>4</td><td>18.18%</td><td>36.36%</td><td>|||||||</td></tr>
<tr><td>6</td><td>1</td><td>5</td><td>9.09%</td><td>45.45%</td><td>|||</td></tr>
<tr><td>8</td><td>1</td><td>6</td><td>9.09%</td><td>54.55%</td><td>|||</td></tr>
<tr><td>10</td><td>4</td><td>10</td><td>36.36%</td><td>90.91%</td><td>||||||||||||||</td></tr>
<tr><td>20</td><td>1</td><td>11</td><td>9.09%</td><td>100.00%</td><td>|||</td></tr>
</table>

The number of missing values is 39.
The overall count including missing values is 50.
The overall percentage of missing values is 78.00%.

Frequency Distribution of B10 Pers_Mob_use

<table>
<tr><th>B10 Pers_Mob_use</th><th>Count</th><th>Cumulative Count</th><th>Percent</th><th>Cumulative Percent</th><th>Graph of Percent</th></tr>
<tr><td>Missing</td><td>7</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Yes</td><td>9</td><td>9</td><td>20.93%</td><td>20.93%</td><td>||||||||</td></tr>
<tr><td>2 Not sure</td><td>7</td><td>16</td><td>16.28%</td><td>37.21%</td><td>||||||</td></tr>
<tr><td>3 No</td><td>27</td><td>43</td><td>62.79%</td><td>100.00%</td><td>|||||||||||||||||||||||||</td></tr>
</table>

The number of missing values is 7.
The overall count including missing values is 50.
The overall percentage of missing values is 14.00%.

Frequency Distribution of C11 Imp_Mob_Emp

<table>
<tr><th></th><th></th><th>Cumulative</th><th></th><th>Cumulative</th><th>Graph of</th></tr>
<tr><th>C11 Imp_Mob_Emp</th><th>Count</th><th>Count</th><th>Percent</th><th>Percent</th><th>Percent</th></tr>
<tr><td>Missing</td><td>2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Very important</td><td>18</td><td>18</td><td>37.50%</td><td>37.50%</td><td>|||||||||||||||</td></tr>
<tr><td>2 Important</td><td>13</td><td>31</td><td>27.08%</td><td>64.58%</td><td>||||||||||</td></tr>
<tr><td>3 Not so important</td><td>8</td><td>39</td><td>16.67%</td><td>81.25%</td><td>||||||</td></tr>
<tr><td>4 Not important at all</td><td>9</td><td>48</td><td>18.75%</td><td>100.00%</td><td>|||||||</td></tr>
</table>

The number of missing values is 2.
The overall count including missing values is 50.
The overall percentage of missing values is 4.00%.

Frequency Distribution of C12 Imp_Mob_Man

<table>
<tr><th></th><th></th><th>Cumulative</th><th></th><th>Cumulative</th><th>Graph of</th></tr>
<tr><th>C12 Imp_Mob_Man</th><th>Count</th><th>Count</th><th>Percent</th><th>Percent</th><th>Percent</th></tr>
<tr><td>Missing</td><td>2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Very important</td><td>19</td><td>19</td><td>39.58%</td><td>39.58%</td><td>|||||||||||||||</td></tr>
<tr><td>2 Important</td><td>20</td><td>39</td><td>41.67%</td><td>81.25%</td><td>||||||||||||||||</td></tr>
<tr><td>3 Not so important</td><td>5</td><td>44</td><td>10.42%</td><td>91.67%</td><td>||||</td></tr>
<tr><td>4 Not important at all</td><td>4</td><td>48</td><td>8.33%</td><td>100.00%</td><td>|||</td></tr>
</table>

The number of missing values is 2.
The overall count including missing values is 50.
The overall percentage of missing values is 4.00%.

Frequency Distribution of C13 Ave_hrs_use

<table>
<tr><th></th><th></th><th>Cumulative</th><th></th><th>Cumulative</th><th>Graph of</th></tr>
<tr><th>C13 Ave_hrs_use</th><th>Count</th><th>Count</th><th>Percent</th><th>Percent</th><th>Percent</th></tr>
<tr><td>Missing</td><td>20</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>3</td><td>3</td><td>10.00%</td><td>10.00%</td><td>||||</td></tr>
<tr><td>2</td><td>1</td><td>4</td><td>3.33%</td><td>13.33%</td><td>|</td></tr>
<tr><td>3</td><td>2</td><td>6</td><td>6.67%</td><td>20.00%</td><td>||</td></tr>
<tr><td>4</td><td>3</td><td>9</td><td>10.00%</td><td>30.00%</td><td>||||</td></tr>
<tr><td>6</td><td>4</td><td>13</td><td>13.33%</td><td>43.33%</td><td>|||||</td></tr>
<tr><td>7</td><td>1</td><td>14</td><td>3.33%</td><td>46.67%</td><td>|</td></tr>
<tr><td>8</td><td>15</td><td>29</td><td>50.00%</td><td>96.67%</td><td>||||||||||||||||||||</td></tr>
<tr><td>12</td><td>1</td><td>30</td><td>3.33%</td><td>100.00%</td><td>|</td></tr>
</table>

The number of missing values is 20.
The overall count including missing values is 50.
The overall percentage of missing values is 40.00%.

Frequency Distribution of C14 Mob_use_Eff_Prod

<table>
<tr><th></th><th></th><th>Cumulative</th><th></th><th>Cumulative</th><th>Graph of</th></tr>
<tr><th>C14 Mob_use_Eff_Prod</th><th>Count</th><th>Count</th><th>Percent</th><th>Percent</th><th>Percent</th></tr>
<tr><td>Missing</td><td>10</td><td></td><td></td><td></td><td></td></tr>
<tr><td>1 Strongly Agree</td><td>21</td><td>21</td><td>52.50%</td><td>52.50%</td><td>|||||||||||||||||||||</td></tr>
<tr><td>2 Agree</td><td>15</td><td>36</td><td>37.50%</td><td>90.00%</td><td>|||||||||||||||</td></tr>
<tr><td>3 Disagree</td><td>3</td><td>39</td><td>7.50%</td><td>97.50%</td><td>|||</td></tr>
<tr><td>4 Strongly Disagree</td><td>1</td><td>40</td><td>2.50%</td><td>100.00%</td><td>|</td></tr>
</table>

The number of missing values is 10.

The overall count including missing values is 50.
The overall percentage of missing values is 20.00%.

Frequency Distribution of D15 Risk_Man_sys

D15 Risk_Man_sys	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	1				
1 Yes	33	33	67.35%	67.35%	||||||||||||||||||||||||||
2 Not sure	7	40	14.29%	81.63%	|||||
3 No	9	49	18.37%	100.00%	|||||||

The number of missing values is 1.
The overall count including missing values is 50.
The overall percentage of missing values is 2.00%.

Frequency Distribution of D16 Type_Risk_Man

D16 Type_Risk_Man	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	15				
1 Yes	8	8	22.86%	22.86%	|||||||||
2 Not sure	9	17	25.71%	48.57%	||||||||||
3 No	18	35	51.43%	100.00%	||||||||||||||||||||

The number of missing values is 15.
The overall count including missing values is 50.
The overall percentage of missing values is 30.00%.

Frequency Distribution of D17 Risk_Man_ftn

D17 Risk_Man_ftn	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	1				
1 Yes	20	20	40.82%	40.82%	||||||||||||||||
2 Not sure	18	38	36.73%	77.55%	||||||||||||||
3 No	11	49	22.45%	100.00%	||||||||

The number of missing values is 1.
The overall count including missing values is 50.
The overall percentage of missing values is 2.00%.

Frequency Distribution of D18 Type_Risk_Man_ftn

D18 Type_Risk_Man_ftn	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	20				
1 In-house	16	16	53.33%	53.33%	|||||||||||||||||||||
2 Co-sourced	2	18	6.67%	60.00%	||
3 Outsourced	2	20	6.67%	66.67%	||
4 Not sure	10	30	33.33%	100.00%	|||||||||||||

The number of missing values is 20.

The overall count including missing values is 50.
The overall percentage of missing values is 40.00%.

Frequency Distribution of D19 Had_info_sec_breach

D19 Had_info_sec_breach	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	1				
1 Yes	5	5	10.20%	10.20%	||||
2 Not sure	24	29	48.98%	59.18%	|||||||||||||||||||
3 No	20	49	40.82%	100.00%	||||||||||||||||

The number of missing values is 1.
The overall count including missing values is 50.
The overall percentage of missing values is 2.00%.

Frequency Distribution of D20 Nr_such_cases

D20 Nr_such_cases	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	48				
1	2	2	100.00%	100.00%	
	||||||||||||||||||||||||||||||||||||||||				

The number of missing values is 48.
The overall count including missing values is 50.
The overall percentage of missing values is 96.00%.

Frequency Distribution of E21 Exist_Appr_proc

E21 Exist_Appr_proc	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Yes	17	17	34.00%	34.00%	|||||||||||||
2 Not sure	18	35	36.00%	70.00%	||||||||||||||
3 No	15	50	30.00%	100.00%	||||||||||||

Frequency Distribution of E22 Exist_Policy

E22 Exist_Policy	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Yes	15	15	30.00%	30.00%	||||||||||||
2 Not sure	17	32	34.00%	64.00%	|||||||||||||
3 No	18	50	36.00%	100.00%	||||||||||||||

Frequency Distribution of E23 Empl_train

E23 Empl_train	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Yes	6	6	12.00%	12.00%	||||
2 Not sure	9	15	18.00%	30.00%	|||||||

```
3 No                              35          50     70.00%     100.00%   ||||||||||||||||||||||||||||
```

Frequency Distribution of E24 Freq_train

```
                                        Cumulative               Cumulative   Graph of
E24 Freq_train                    Count      Count    Percent       Percent   Percent
Missing                              38
2 Quarterly                           1          1      8.33%         8.33%   |||
4 Annually                            4          5     33.33%        41.67%   |||||||||||||
5 Not sure                            7         12     58.33%       100.00%   |||||||||||||||||||||||
```

The number of missing values is 38.
The overall count including missing values is 50.
The overall percentage of missing values is 76.00%.

Frequency Distribution of E25 Record_ emp_Mob_access

```
                                        Cumulative               Cumulative   Graph of
E25 Record_ emp_Mob_accessCount              Count    Percent       Percent   Percent
1 Yes                                16         16     32.00%        32.00%   ||||||||||||
2 Not sure                           19         35     38.00%        70.00%   |||||||||||||||
3 No                                 15         50     30.00%       100.00%   ||||||||||||
```

Frequency Distribution of E26 Freq_re-eval_Mob_req

```
                                        Cumulative               Cumulative   Graph of
E26 Freq_re-eval_Mob_req          Count      Count    Percent       Percent   Percent
Missing                              30
1 Monthly                             4          4     20.00%        20.00%   ||||||||
2 Quarterly                           3          7     15.00%        35.00%   ||||||
3 Twice a year                        1          8      5.00%        40.00%   ||
5 Not sure                           12         20     60.00%       100.00%   ||||||||||||||||||||||||
```

The number of missing values is 30.
The overall count including missing values is 50.
The overall percentage of missing values is 60.00%.

Frequency Distribution of E27 Freq_Risk_Reg_update

```
                                        Cumulative               Cumulative   Graph of
E27 Freq_Risk_Reg_update          Count      Count    Percent       Percent   Percent
Missing                               1
1 Monthly                             3          3      6.12%         6.12%   ||
2 Quarterly                          25         28     51.02%        57.14%   ||||||||||||||||||||
3 Twice a year                        1         29      2.04%        59.18%   |
4 Annually                            6         35     12.24%        71.43%   ||||
5 Not sure                           14         49     28.57%       100.00%   |||||||||||
```

The number of missing values is 1.
The overall count including missing values is 50.
The overall percentage of missing values is 2.00%.

Frequency Distribution of E28 Exist_Risk_Man_Comm

E28 Exist_Risk_Man_Comm	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
1 Yes	32	32	64.00%	64.00%	|||||||||||||||||||||||||
2 Not sure	7	39	14.00%	78.00%	|||||
3 No	11	50	22.00%	100.00%	||||||||

Frequency Distribution of E29 Freq_Risk_Man_meet

E29 Freq_Risk_Man_meet	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	9				
1 Monthly	2	2	4.88%	4.88%	|
2 Quarterly	25	27	60.98%	65.85%	||||||||||||||||||||||||
4 Annually	2	29	4.88%	70.73%	|
5 Not sure	12	41	29.27%	100.00%	|||||||||||

The number of missing values is 9.
The overall count including missing values is 50.
The overall percentage of missing values is 18.00%.

Frequency Distribution of F30 Man_Risk_iro_Mob

F30 Man_Risk_iro_Mob	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	14				
1 Very Good	6	6	16.67%	16.67%	||||||
2 Good	7	13	19.44%	36.11%	|||||||
3 Fairly good	10	23	27.78%	63.89%	|||||||||||
4 Poor	13	36	36.11%	100.00%	||||||||||||||

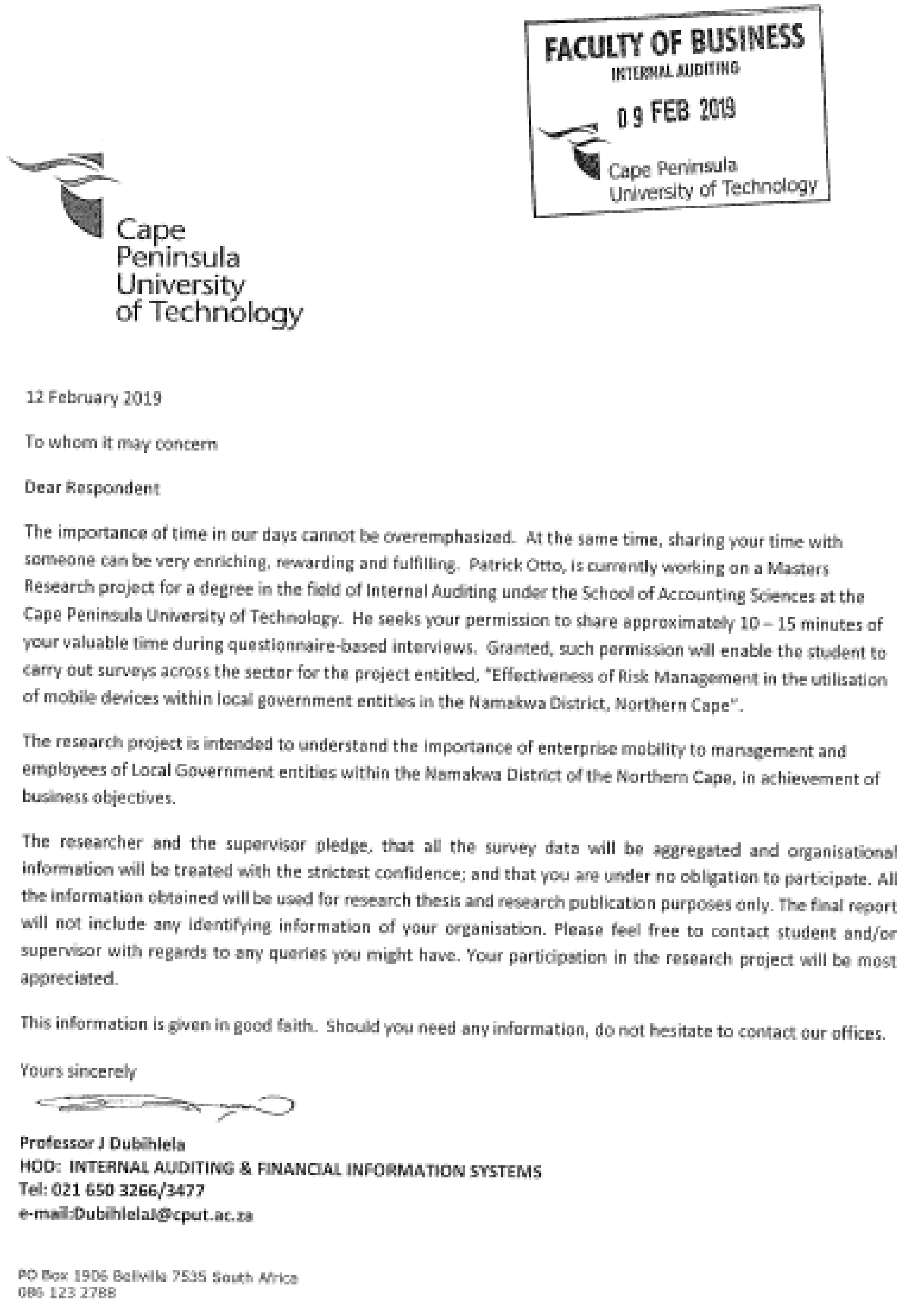
The number of missing values is 14.
The overall count including missing values is 50.
The overall percentage of missing values is 28.00%.

Frequency Distribution of F31 Effectiv_Risk_Man

F31 Effectiv_Risk_Man	Count	Cumulative Count	Percent	Cumulative Percent	Graph of Percent
Missing	9				
1 Strongly Agree	4	4	9.76%	9.76%	|||
2 Agree	25	29	60.98%	70.73%	||||||||||||||||||||||||
3 Disagree	11	40	26.83%	97.56%	||||||||||
4 Strongly Disagree	1	41	2.44%	100.00%	|

The number of missing values is 9.
The overall count including missing values is 50.
The overall percentage of missing values is 18.00%.

APPENDIX B: FACULTY OF BUSINESS AND MANAGEMENT SCIENCE: RESEARCH LETTER



FACULTY OF BUSINESS
INTERNAL AUDITING
09 FEB 2019
Cape Peninsula
University of Technology

Cape
Peninsula
University
of Technology

12 February 2019

To whom it may concern

Dear Respondent

The importance of time in our days cannot be overemphasized. At the same time, sharing your time with someone can be very enriching, rewarding and fulfilling. Patrick Otto, is currently working on a Masters Research project for a degree in the field of Internal Auditing under the School of Accounting Sciences at the Cape Peninsula University of Technology. He seeks your permission to share approximately 10 – 15 minutes of your valuable time during questionnaire-based interviews. Granted, such permission will enable the student to carry out surveys across the sector for the project entitled, "Effectiveness of Risk Management in the utilisation of mobile devices within local government entities in the Namakwa District, Northern Cape".

The research project is intended to understand the importance of enterprise mobility to management and employees of Local Government entities within the Namakwa District of the Northern Cape, in achievement of business objectives.

The researcher and the supervisor pledge, that all the survey data will be aggregated and organisational information will be treated with the strictest confidence; and that you are under no obligation to participate. All the information obtained will be used for research thesis and research publication purposes only. The final report will not include any identifying information of your organisation. Please feel free to contact student and/or supervisor with regards to any queries you might have. Your participation in the research project will be most appreciated.

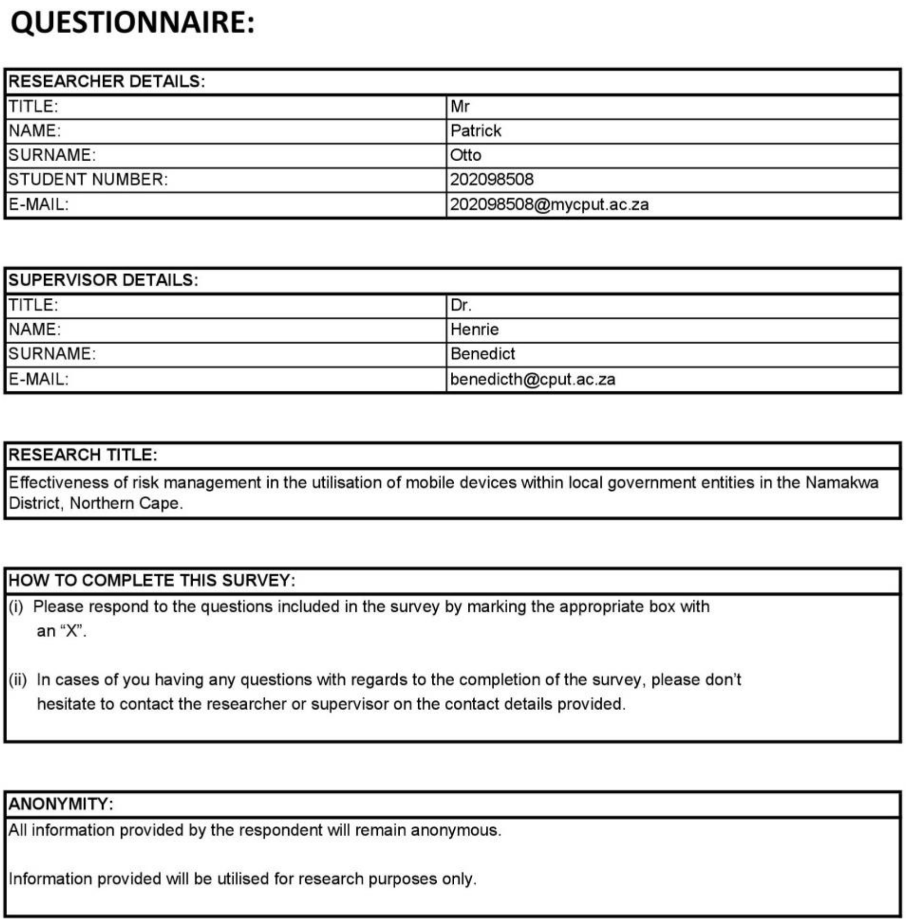
This information is given in good faith. Should you need any information, do not hesitate to contact our offices.

Yours sincerely

Professor J Dubihlela
HOD: INTERNAL AUDITING & FINANCIAL INFORMATION SYSTEMS
Tel: 021 650 3266/3477
e-mail:Dubihlelal@cput.ac.za

PO Box 1906 Bellville 7535 South Africa
086 123 2788

APPENDIX C: RESEARCH QUESTIONNAIRE



QUESTIONNAIRE:

RESEARCHER DETAILS:	
TITLE:	Mr
NAME:	Patrick
SURNAME:	Otto
STUDENT NUMBER:	202098508
E-MAIL:	202098508@mycput.ac.za

SUPERVISOR DETAILS:	
TITLE:	Dr.
NAME:	Henrie
SURNAME:	Benedict
E-MAIL:	benedicth@cput.ac.za

RESEARCH TITLE:

Effectiveness of risk management in the utilisation of mobile devices within local government entities in the Namakwa District, Northern Cape.

HOW TO COMPLETE THIS SURVEY:

(i) Please respond to the questions included in the survey by marking the appropriate box with an “X”.

(ii) In cases of you having any questions with regards to the completion of the survey, please don’t hesitate to contact the researcher or supervisor on the contact details provided.

ANONYMITY:

All information provided by the respondent will remain anonymous.

Information provided will be utilised for research purposes only.

SECTION A – RESPONDENT AND ENTERPRISE INFORMATION

1. What is your gender?

Male		1
Female		2

2. Which age category do you fall in?

19 – 25		1
26 – 35		2
36 – 45		3
46 – 55		4
56 – 65		5

3. How many years of experience do you have? (Please complete the number of years or months in the applicable box below)

Years		1
Months		2

4. How many people are employed within your organisation? (Please complete the number of employees in the box below)

Number of employees		1

5. At which level are your current position?

Senior Management		1		
Middle Management		2		
Non Management		3		
Other		4	Please specify:	

SECTION B – MOBILE DEVICE CONNECTIONS TO ENTERPRISE NETWORKS

6. Does your organisation permit the connection with mobile devices (i.e. Laptops, Mobile Smartphones, Tablets, etc.) to the enterprise's network in order to access organisation's information?

Yes		1
Not sure		2
No		3

If your answer (Question 6) is <u>No</u> or <u>Not Sure</u>, please proceed to Question 11.

7. If yes (Question 6), which mobile devices do you make use of? (Tick all the appropriate devices utilised below)

Laptops		1		
Mobile Smartphones		2		
Tablets		3		
Other		4	Please specify:	
Not applicable		5		

8. Are you allowed to access organisational information remotely when away from the office?

Yes		1
No		2
Not applicable		3

9. How many years have your organisation been permitting the connection of mobile devices to the enterprise's network? (Please complete number of years or months if applicable in the box below)

Years		1
Months		2
Not sure		3
Not used		4

10. Does your organisation allow your personal mobile device to be connected to the enterprise's network?

Yes		1
Not sure		2
No		3

SECTION C – MOBILE DEVICE CONNECTIONS TO ENTERPRISE NETWORKS (EMPLOYEES)

11. Access with my mobile device to the corporate network is:

Very important		1
Important		2
Not so important		3
Not important at all		4

12. In order to deliver on business objectives our management deem access with mobile devices to the corporate network as:

Very important		1
Important		2
Not so important		3
Not important at all		4

13. How many hours per day on average do you spend on accessing business information on your enterprise's network using a mobile device? (Please complete number of hours or minutes if applicable in the box below)

Hours		1
Minutes		2
Not applicable		3

14. Access with my mobile device to the corporate network enhance efficiency and productivity:

Strongly Agree		1
Agree		2
Disagree		3
Strongly Disagree		4
Not applicable		5

SECTION D – MOBILE DEVICE CONNECTIONS TO ENTERPRISE NETWORKS (RISK MANAGEMENT)

15. Does your organisation have a risk management system?

Yes		1
Not sure		2
No		3

16. If yes (Question 15), is it an electronic system (not an Excel spreadsheet)?

Yes		1
Not sure		2
No		3
Not applicable		4

17. Does your enterprise have a risk management function to identify, assess and monitor risks pertaining to the usage of mobile devices (i.e. compliance, privacy, physical security and information security risks)

Yes		1
Not sure		2
No		3

18. If yes (Question 17), is it an in-house, outsourced or co-sourced risk management function?

In-house		1
Co-sourced		2
Outsourced		3
Not sure		4
Not applicable		5

19. Have your organisation experienced a breach in terms of information security since permitting the connection of mobile devices to the enterprise's network?

Yes		1
Not sure		2
No		3

20. If yes (Question 19), how many times have your organisation experienced a breach in terms of information security as a result of the connection of mobile devices to enterprise networks within the last 12 months? (Please complete the number of times, if applicable in the box below)

Number of times		1
Not sure		2
Not applicable		3

SECTION E – MOBILE DEVICE CONNECTIONS TO ENTERPRISE NETWORKS (MITIGATIONS)

21. Does your organisation have a formal process in place in terms of the approval of access requests pertaining to the connection of mobile devices to the enterprise's network?

Yes		1
Not sure		2
No		3

22. Does your organisation have a formal policy and / or procedure developed to guide employees with regards to mobile devices connected to the enterprise's network?

Yes		1
Not sure		2
No		3

23. Does your organisation provide formal training on a frequent basis to employees with regards to mobile device connections to the enterprise's network in order to create security awareness?

Yes		1
Not sure		2
No		3

24. If yes (Question 23), how often does this training happen?

Monthly		1
Quarterly		2
Twice a year		3
Annually		4
Not sure		5
Not applicable		6

25. Does your organisation maintain formal records of all employees approved to have access to the enterprise's network with mobile devices?

Yes		1
Not sure		2
No		3

26. If yes (Question 25), how often do they evaluate whether such access is still a requirement in line with initial approval?

Monthly		1
Quarterly		2
Twice a year		3
Annually		4
Not sure		5
Not applicable		6

27. How often is risk registers updated within your organisation?

Monthly		1
Quarterly		2
Twice a year		3
Annually		4
Not sure		5
Not applicable		6

28. Does your organisation have a Risk Management Committee where the management of organisation risks are discussed?

Yes		1
Not sure		2
No		3

29. How often does the Risk Management Committee meet?

Monthly		1
Quarterly		2
Twice a year		3
Annually		4
Not sure		5
Not applicable		6

SECTION F – MANAGEMENT OF RISKS WITHIN YOUR ENTERPRISE

30. Risks relating to mobile device connections to my enterprise network are managed:

Very Good		1
Good		2
Fairly good		3
Poor		4
Not applicable		5

31. Risk management within my enterprise is effective.

Strongly Agree		1
Agree		2
Disagree		3
Strongly Disagree		4
Not applicable		5

SECTION G – THANK YOU

Thank you for your time and effort in completing the survey pertaining to the academic research study.

Please e-mail completed survey to 202098508@mycput.ac.za

Please complete the following fields with information pertaining to yourself:

TITLE: ………………………………………………………………………………

NAME: ………………………………………………………………………………

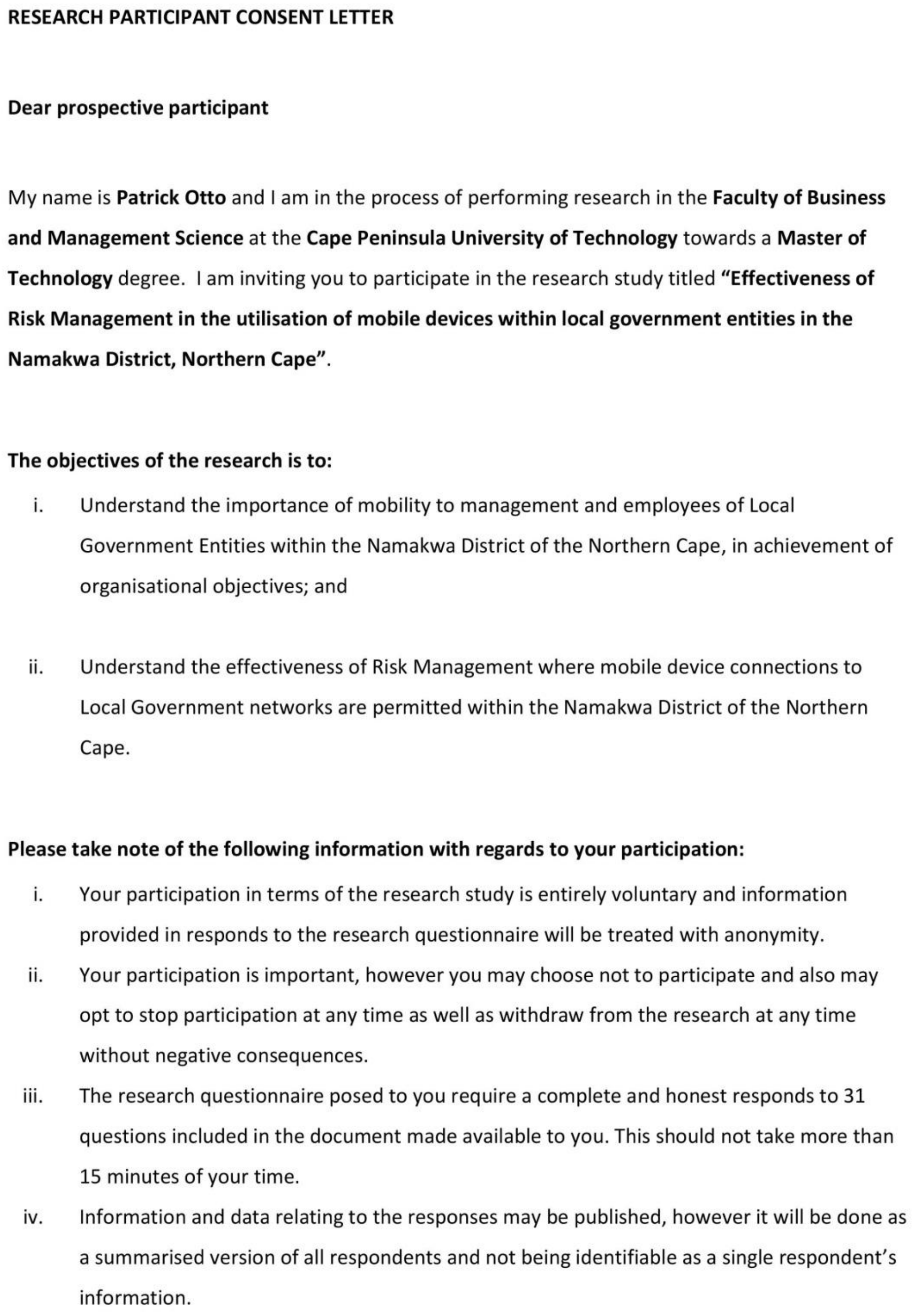
SURNAME: ………………………………………………………………………………

CONTACT NUMBER: ………………………………………………………………………………

CITY & PROVINCE: ………………………………………………………………………………

DATE COMPLETED: ………………………………………………………………………………

APPENDIX D: RESEARCH PARTICIPATION CONSENT LETTER



RESEARCH PARTICIPANT CONSENT LETTER

Dear prospective participant

My name is **Patrick Otto** and I am in the process of performing research in the **Faculty of Business and Management Science** at the **Cape Peninsula University of Technology** towards a **Master of Technology** degree. I am inviting you to participate in the research study titled **"Effectiveness of Risk Management in the utilisation of mobile devices within local government entities in the Namakwa District, Northern Cape"**.

The objectives of the research is to:

i. Understand the importance of mobility to management and employees of Local Government Entities within the Namakwa District of the Northern Cape, in achievement of organisational objectives; and

ii. Understand the effectiveness of Risk Management where mobile device connections to Local Government networks are permitted within the Namakwa District of the Northern Cape.

Please take note of the following information with regards to your participation:

i. Your participation in terms of the research study is entirely voluntary and information provided in responds to the research questionnaire will be treated with anonymity.

ii. Your participation is important, however you may choose not to participate and also may opt to stop participation at any time as well as withdraw from the research at any time without negative consequences.

iii. The research questionnaire posed to you require a complete and honest responds to 31 questions included in the document made available to you. This should not take more than 15 minutes of your time.

iv. Information and data relating to the responses may be published, however it will be done as a summarised version of all respondents and not being identifiable as a single respondent's information.

v. The results of the research study will be utilised for academic purposes only and anonymously included in the master’s thesis document and may also be published in an academic journal as a summary of information received from all respondents.

Thank you for taking the time to read through the information provided above and availing yourself to participate in this research study being conducted.

Yours Faithfully

Patrick Otto

CONSENT TO PARTICIPATE IN THIS RESEARCH STUDY

I …………………………………………………………………………………………………… (participant name and surname), confirmed that the researcher obtained my consent to partake in this research study and provided me with information relating to participation. I understand that participation is entirely voluntary and information provided in responds to the research questionnaire will be treated with anonymity. The results of the research study will be utilised for academic purposes only and may be published in an academic journal as a summary of information received from all respondents and not being identifiable as a single respondent’s information. I am aware that information of the study will be anonymously included into the master’s thesis document.

Participant signature ………

Date of completion ……

Note: Please sent completed **Research Participation Consent Letter** via e-mail to **202098508@mycput.ac.za**.

APPENDIX E: DATA CODING

i. Data coding – Gender

CODE	FACTOR
1	Male
2	Female

ii. Data coding – Age Category

CODE	FACTOR
1	19 – 25
2	26 – 35
3	36 – 45
4	46 – 55
5	56 – 65

iii. Data coding – Level of Seniority

CODE	FACTOR
1	Senior Management
2	Middle Management
3	Non-Management

iv. Data coding – Organisation permitting the connection with mobile devices

CODE	FACTOR
1	Yes
2	Not sure
3	No

v. Data coding – Type of mobile devices utilised

CODE	FACTOR
1	Laptops
2	Smartphones
3	Tablets
4	Other

vi. Data coding – Remote access allowed by the organisation

CODE	FACTOR
1	Yes
2	No

vii. Data coding – Personal mobile device connections permitted

CODE	FACTOR
1	Yes
2	Not sure
3	No

viii. Data coding – Importance of access with mobile devices to corporate network for Employees

CODE	FACTOR
1	Very important
2	Important
3	Not so important
4	Not important at all

ix. Data coding – Importance of mobile device connections according to Management during deliverance on business objectives

CODE	FACTOR
1	Very important
2	Important
3	Not so important
4	Not important at all

x. Data coding – Mobile device connections results in enhanced efficiency and productivity

CODE	FACTOR
1	Strongly agree
2	Agree
3	Disagree
4	Strongly disagree

xi. Data coding – Existence of a risk management system within organisations

CODE	FACTOR
1	Yes
2	Not sure
3	No

xii. Data coding – Electronic risk management system

CODE	FACTOR
1	Yes
2	Not sure
3	No

xiii. Data coding – Existence of a risk management function

CODE	FACTOR
1	Yes
2	Not sure
3	No

xiv. Data coding – Type of risk management function

CODE	FACTOR
1	In-house
2	Co-sourced
3	Outsourced
4	Not sure

xv. Data coding – Breach in information security experienced since permitting mobile devices connections

CODE	FACTOR
1	Yes
2	Not sure
3	No

xvi. Data coding – Existence of a formal approval process pertaining to mobile device connections

CODE	FACTOR
1	Yes
2	Not sure
3	No

xvii. Data coding – Existence of a formal policy and/or procedure to provide guidance to employees with regards to mobile device connections

CODE	FACTOR
1	Yes
2	Not sure
3	No

xviii. Data coding – Formal training performed on a frequent basis to employees with regards to mobile device connections to create security awareness

CODE	FACTOR
1	Yes
2	Not sure
3	No

xix. Data coding – Frequency of training performed to create security awareness

CODE	FACTOR
1	Monthly
2	Quarterly
3	Twice a year
4	Annually
5	Not sure

xx. Data coding – Existence of a formal records of all employees approved to have access to the organisational network with mobile devices

CODE	FACTOR
1	Yes
2	Not sure
3	No

xxi. Data coding – Frequency of evaluation of mobile device access subsequent to initial approval

CODE	FACTOR
1	Monthly
2	Quarterly
3	Twice a year
4	Annually
5	Not sure

xxii. Data coding – Frequency of updating risk registers

CODE	FACTOR
1	Monthly
2	Quarterly
3	Twice a year
4	Annually
5	Not sure

xxiii. Data coding – Existence of a risk management committee

CODE	FACTOR
1	Yes
2	Not sure
3	No

xxiv. Data coding – Frequency of risk management committee meetings

CODE	FACTOR
1	Monthly
2	Quarterly
3	Twice a year
4	Annually
5	Not sure

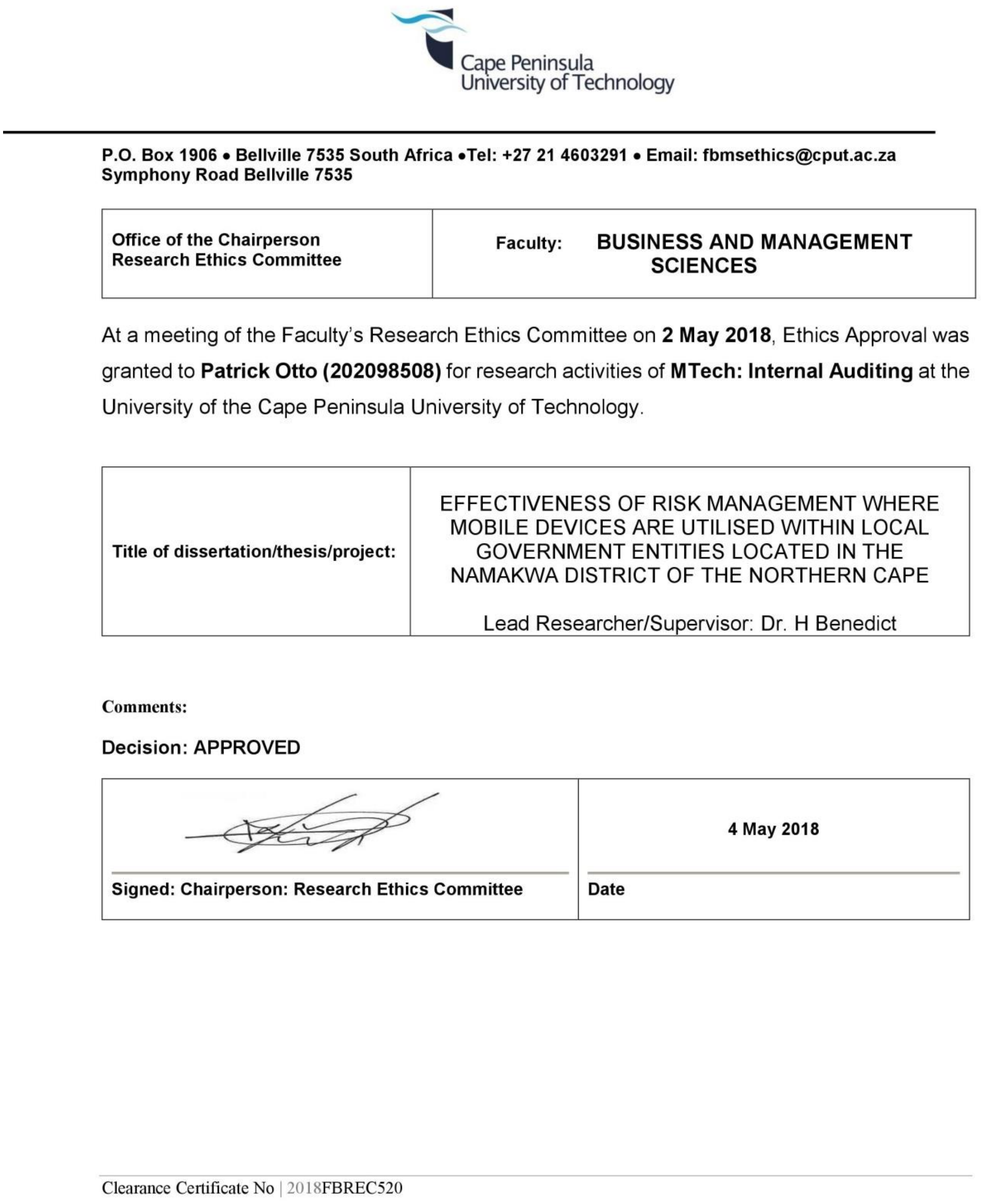
xxv. Data coding – Mobile device related risks are managed

CODE	FACTOR
1	Very good
2	Good
3	Fairly good
4	Poor

xxvi. Data coding – Risk management within the organisation is effective

CODE	FACTOR
1	Strongly agree
2	Agree
3	Disagree
4	Strongly disagree

APPENDIX F: ETHICAL CLEARANCE



Cape Peninsula
University of Technology

P.O. Box 1906 • Bellville 7535 South Africa •Tel: +27 21 4603291 • Email: fbmsethics@cput.ac.za
Symphony Road Bellville 7535

Office of the Chairperson **Research Ethics Committee**	**Faculty: BUSINESS AND MANAGEMENT SCIENCES**

At a meeting of the Faculty's Research Ethics Committee on **2 May 2018**, Ethics Approval was granted to **Patrick Otto (202098508)** for research activities of **MTech: Internal Auditing** at the University of the Cape Peninsula University of Technology.

Title of dissertation/thesis/project:	EFFECTIVENESS OF RISK MANAGEMENT WHERE MOBILE DEVICES ARE UTILISED WITHIN LOCAL GOVERNMENT ENTITIES LOCATED IN THE NAMAKWA DISTRICT OF THE NORTHERN CAPE Lead Researcher/Supervisor: Dr. H Benedict

Comments:

Decision: APPROVED

	4 May 2018
Signed: Chairperson: Research Ethics Committee	**Date**

Clearance Certificate No | 2018FBREC520

APPENDIX G: GRAMMARIAN LETTER

22 Krag Street
Napier
7270
Overberg
Western Cape

4 February 2020

TECHNICAL & LANGUAGE EDITING

Cheryl M. Thomson

EFFECTIVENESS OF RISK MANAGEMENT IN THE UTILISATION OF MOBILE DEVICES WITHIN LOCAL GOVERNMENT ENTITIES IN THE NAMAKWA DISTRICT, NORTHERN CAPE

Supervisor: Dr H Benedict

This is to confirm that I, Cheryl Thomson, executed the language and technical editing of the above-titled Master's dissertation of PATRICK OTTO, student number 202098508, at the CAPE PENINSULA UNIVERSITY OF TECHNOLOGY in preparation for submission of this dissertation for assessment.

Yours faithfully

CHERYL M. THOMSON

Email: cherylthomson2@gmail.com

Cell: 0826859545