



**UNIVERSITY OF KWAZULU-NATAL**

College of Law and Management Studies

School of Management, Information Technology and Governance

**FACTORS TO CONSIDER WHEN DEVELOPING AN ORGANISATION-WIDE  
BRING YOUR OWN DEVICE (BYOD) STRATEGY FOR ADOPTION**

A research dissertation submitted in partial fulfilment of the requirements for the degree of

Master of Commerce

in

Information Systems & Technology

By

SOLOMON OLUWASEUN OMOKEHINDE

214577345

Supervisor:

Mr. Ashley Marimuthu

2019



## DECLARATION

I, Solomon Oluwaseun Omokehinde declare that:

- i. The research reported in this thesis, except where otherwise indicated, and is my original work.
- ii. This thesis has not been submitted for any degree or examination at any other University.
- iii. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
- iv. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
  - a) Their words have been re-written, but the general information attributed to them has been referenced;
  - b) Where their exact words have been used, their writing has been placed inside quotation marks and referenced.
- v. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.
- vi. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed:



S. O. Omokehinde

214577345

## **ACKNOWLEDGMENTS**

I wish to express my appreciation and sincere gratefulness to the following parties, without whose support, this research would not have been possible:

- Mr. Ashley Marimuthu, in his role as my research supervisor, for his heartfelt assistance in demystifying complex concepts, and his patience during the learning process,
- My Dad, Dr. J. O. Omokehinde for funding the education of our family,
- My family for their support during the long days and even longer nights,
- My friends, Eniola Folarin, Eniola Lisoyi, Jide Enigbokan, Chika Chukwuma, Arinze Obiora, Taiwo Ajadi and Muzi Simelane for their support during the course of the program,
- And finally, the people who have taken the time to support and share their experiences.

## ABSTRACT

The use of a mobile device has now become a part of humans' day-to-day activities; this also includes activities in the workplace. Organisations are learning of their workforce tenacious desire to use their personally owned mobile devices to carry out work activities; hence, a large number of corporate employees are requesting for the company's Information Technology (IT) division to make provision for these devices. Organisations have come to terms with the reality of their inability to prevent the utilisation of mobile artefacts (smartphones and tablets) for both personal and work purposes, but they are expected to know how to regulate how these devices impact its network ecosystem. The sudden surge of Bring Your Own Device (BYOD) within an organisation nonetheless, emanates, primarily because of the global growth in the use of mobile artefacts (smartphones and tablets), combined with the emerging acceptance and the universal presence of media-sharing tools. However, evidence shows that the growth in the proliferation of employees' mobile devices within the workplace can cause a significant information security problem that many organisations are not equipped to address. This study entailed an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets within the workplace. The overall aim of the study was to document a set of factors that needs to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of the organisational IT infrastructure. The study adopted a qualitative research approach utilising a non-probability (purposive) sampling technique. Interviews were used to elicit information on the factors to consider when developing a BYOD strategy for adoption, the interviews were conducted among fourteen (14) senior executives in various organisations in eThekweni Municipal Region, South Africa that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. The data collected were analysed using a thematic analysis. From the study's findings, the key factors that IT managers need to consider when implementing strategies for using personal devices (smartphones and tablets) within an organisation are framed into a selected set of four larger components. These four components; policy development, employee education, data security and mobile work-learning, further revealed that sub-factors such as systems management, policy review, authorised usage, limitations of liability, data segregation, data encryption, use of a strong password for the following types of authentication (device, user, and container), virtual private network, employee education and training, ease of communication and micro-app development are considered as important factors when it concerns the development of a BYOD strategy in an organisation.

# TABLE OF CONTENTS

<b>DECLARATION</b> .....	<b>III</b>
<b>ACKNOWLEDGMENTS</b> .....	<b>IV</b>
<b>ABSTRACT</b> .....	<b>V</b>
<b>TABLE OF CONTENTS</b> .....	<b>VI</b>
<b>LIST OF FIGURES</b> .....	<b>IX</b>
<b>LIST OF TABLES</b> .....	<b>X</b>
<b>LIST OF ACRONYMS</b> .....	<b>XI</b>
<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 INTRODUCTION .....	1
1.2 BACKGROUND OF THE STUDY .....	1
1.3 RESEARCH PROBLEM .....	3
1.4 RESEARCH QUESTIONS.....	4
1.5 RESEARCH OBJECTIVES .....	4
1.6 SIGNIFICANCE OF THE STUDY.....	5
1.7 RESEARCH METHODOLOGY .....	5
1.7.1 <i>Research Approach</i> .....	6
1.7.2 <i>Research Design</i> .....	6
1.7.3 <i>Study Site and Target Population</i> .....	6
1.7.4 <i>Sampling Method</i> .....	6
1.7.5 <i>Data Collection Method</i> .....	7
1.7.6 <i>Data Analysis</i> .....	7
1.8 LIMITATION OF THE STUDY .....	7
1.9 STRUCTURE OF DISSERTATION.....	8
1.10 CONCLUSION .....	8
<b>CHAPTER 2: LITERATURE REVIEW</b> .....	<b>9</b>
2.1 INTRODUCTION .....	9
2.1.1 <i>Introduction to Bring Your Own Device</i> .....	9
2.2 THEORETICAL REVIEW ON BYOD .....	10
2.2.1 <i>Benefits of Implementing a BYOD Strategy</i> .....	11
2.2.2 <i>Challenges of Adopting a BYOD Strategy</i> .....	13
2.2.3 <i>Telecommunications Industry in South Africa</i> .....	14
2.2.4 <i>BYOD Adoption within the IT Industry in South-Africa</i> .....	14
2.3 POLICY FRAMEWORK AND BYOD .....	16
2.3.1 <i>Factors to be considered in the development of the BYOD policy framework</i> .....	17

2.4	DATA SECURITY AND BYOD.....	19
2.4.1	<i>Factors to ensure that Data is secured in a BYOD Culture.....</i>	20
2.5	EMPLOYEE EDUCATION AND BYOD.....	21
2.5.1	<i>Factors to Address Employee Education in a BYOD Culture .....</i>	21
2.6	MOBILE LEARNING IN ORGANISATIONS .....	25
2.6.1	<i>Factors Involved in Designing Learning Experiences.....</i>	28
2.7	CONCEPTUAL FRAMEWORK FOR DEVELOPING A BYOD STRATEGY .....	30
2.8	VALIDATING THE CONCEPTUAL FRAMEWORK .....	32
2.9	CRITIQUE .....	33
<b>CHAPTER 3: RESEARCH METHODOLOGY .....</b>		<b>35</b>
3.1	INTRODUCTION .....	35
3.2	RESEARCH APPROACH .....	35
3.3	RESEARCH DESIGN.....	35
3.4	RESEARCH METHOD .....	36
3.5	RESEARCH SITE AND SETTING .....	37
3.6	POPULATION OF THE STUDY .....	38
3.7	SAMPLING AND SAMPLING TECHNIQUE .....	38
3.8	SAMPLE AND SAMPLE SIZE .....	39
3.9	PARTICIPANTS’ DEMOGRAPHICS .....	40
3.10	DATA COLLECTION .....	40
3.10.1	<i>Interview.....</i>	41
3.10.2	<i>Interview Schedule.....</i>	41
3.11	ENSURING RELIABILITY AND VALIDITY .....	42
3.11.1	<i>Triangulation.....</i>	42
3.11.2	<i>Credibility (Internal Validity).....</i>	43
3.11.3	<i>Transferability (External Validity) .....</i>	43
3.11.4	<i>Dependability (Reliability) .....</i>	43
3.11.5	<i>Confirmability (Objectivity).....</i>	44
3.12	DATA ANALYSIS .....	45
3.12.1	<i>Thematic Analysis Phases.....</i>	45
3.12.2	<i>Themes of Analysis .....</i>	46
3.13	ETHICAL CONSIDERATION.....	47
3.14	CONCLUSION.....	48
<b>CHAPTER 4: DATA PRESENTATION AND ANALYSIS.....</b>		<b>49</b>
4.1	INTRODUCTION .....	49
4.2	CONCEPTUAL FRAMEWORK .....	49
4.3	POLICY.....	51

4.3.1	<i>Authorised Usage</i> .....	53
4.3.2	<i>Systems Management</i> .....	56
4.3.3	<i>Policy Review</i> .....	58
4.3.4	<i>Limitations of Liability</i> .....	60
4.4	SECURITY OF DATA.....	61
4.4.1	<i>Segregating Data</i> .....	63
4.4.2	<i>Data Encryption</i> .....	65
4.4.3	<i>Use of a Strong Password for (Device, User, and Container Authentication)</i> .....	67
4.4.4	<i>Virtual Private Network</i> .....	69
4.5	EMPLOYEE EDUCATION .....	71
4.6	MOBILE LEARNING .....	73
4.7	SUMMARY OF RESEARCH FINDINGS .....	75
4.8	CONCLUSION.....	76
<b>CHAPTER 5: SUMMARY, RECOMMENDATIONS AND CONCLUSION .....</b>		<b>77</b>
5.1	INTRODUCTION .....	77
5.2	SUMMARY OF DISSERTATION .....	77
5.3	SUMMARY OF RESEARCH FINDINGS .....	79
5.4	RECOMMENDATIONS OF RESEARCH FINDINGS .....	81
5.5	LIMITATIONS AND RECOMMENDATIONS FOR FURTHER RESEARCH.....	86
5.5.1	<i>Sampling Procedure</i> .....	86
5.5.2	<i>Exclusions</i> .....	86
5.5.3	<i>Future Research</i> .....	86
5.6	CONCLUSION.....	87
<b>REFERENCES.....</b>		<b>89</b>
<b>APPENDICES.....</b>		<b>95</b>
APPENDIX A: ETHICAL CLEARANCE LETTER.....		95
APPENDIX B: INFORMED CONSENT DOCUMENT .....		96
APPENDIX C: QUESTIONNAIRE .....		98
APPENDIX D: INTERVIEW PROTOCOL .....		103
APPENDIX E: PROOF OF EDITING LETTER FROM THE EDITOR .....		111
APPENDIX F: GATEKEEPER LETTERS .....		112



## LIST OF FIGURES

FIGURE 2-1: SCHEMATIC DIAGRAM OF THE CONCEPTUAL FRAMEWORK CONCERNING FACTORS FOR DEVELOPING BYOD STRATEGY .....	30
FIGURE 4-1: SCHEMATIC DIAGRAM OF THE ADOPTED CONCEPTUAL FRAMEWORK CONCERNING FACTORS FOR DEVELOPING BYOD STRATEGY .....	50
FIGURE 4-2: POLICY DEVELOPMENT FACTORS AND BYOD I.....	51
FIGURE 4-3: POLICY DEVELOPMENT FACTORS AND BYOD II .....	52
FIGURE 4-4: SECURITY OF DATA FACTORS AND BYOD I.....	61
FIGURE 4-5: SECURITY OF DATA FACTORS AND BYOD II .....	61
FIGURE 4-6: EMPLOYEE EDUCATION FACTORS AND BYOD .....	70
FIGURE 4-7: MOBILE LEARNING IN ORGANISATIONS AND BYOD.....	72
FIGURE 5-1: ADJUSTED CONCEPTUAL FRAMEWORK CONCERNING FACTORS FOR CONSIDERATION WHEN DEVELOPING BYOD STRATEGY MODEL INTEGRATION WITHIN AN ORGANISATION.....	78

## LIST OF TABLES

TABLE 4-1: FACTORS TO CONSIDER WHEN ADOPTING A POLICY FOR ACCEPTABLE AND RESTRICTED MOBILE USAGE IN AN ORGANISATION.....	51
TABLE 4-2: FACTORS THAT ARE RESPONSIBLE FOR SAFEGUARDING SENSITIVE INFORMATION THAT IS ACCESSED ON MOBILE DEVICES THROUGHOUT AN ORGANISATION.....	60
TABLE 5-1: DETAILED DIRECTION FOR DEVELOPING A BYOD POLICY.....	81
TABLE 5-2: DETAILED GUIDE TO ENSURE THE SECURITY OF DATA IN A BYOD ORGANISATION .....	82
TABLE 5-3: HOW TO RAISE EMPLOYEE EDUCATION ON SAFETY STANDARDS WHEN USING PERSONAL DEVICES WITHIN THE ORGANISATION .....	83
TABLE 5-4: DETAILS TO DESIGNING LEARNING EXPERIENCES IN A BYOD CULTURE .....	84

## LIST OF ACRONYMS

BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CIO	Chief Information Officer
CKO	Chief Knowledge Officer
CTO	Chief Technology Officer
EMR	Electronic Medical Record
HR	Human Resource
HTTP	Hypertext Transfer Protocol
IDC	International Data Centre
ICT	Information and Communications Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MD	Managing Director
MDM	Mobile Device Management
NFC	Near Field Communication
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SMS	Short Message Service
SDK	Software Development Kit
TOE	Technology Organisation Environment
URL	Uniform resource Locator
VM	Virtual machine
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WI-FI	Wireless Fidelity
WWW	World Wide Web



# CHAPTER 1: INTRODUCTION

## 1.1 Introduction

According to Radicati (2016), mobile artefacts such as tablets, phones and notebooks have experienced a significant rise over the last decade. He further claimed that there were over 6.1 billion mobile device users globally in 2016, and by the end of 2020, the total number of mobile users worldwide is projected to grow to over 6.9 billion (Radicati, 2016). With mobile devices progressively fitting into our everyday lives, organisations are discovering that their employees require their portable devices to help conduct work activities. Similarly, corporate personnel are also reaching out to internal IT division to make provision for their mobile devices. Organisations have not only recognised that they are not able to halt the use of electronic devices for both personal and work purposes but, they must understand how best to regulate the proliferation of these devices (EY, 2013).

The swift rise of the term Bring Your Own Device (BYOD) originates from the increase of mobile artefacts (smartphones and tablets) as a technological tool together with the upward pervasion and popularity of file-sharing technologies. Organisations are searching for leaner ways to save capital on computing infrastructure; however, on the other way around, this has produced a massive information security problem that most organisations are not prepared to control which occasionally make them more exposed (Greener *et al.*, 2015).

BYOD notably influences the existing security standards of guarding the boundary of the organisation by concealing the meaning of that boundary through asset ownership and physical location. With employee devices now being used to access business calendars, business data, business applications and electronic mails, many organisations are faced with how to entirely define the effect of their security model and ascertain adequate actions and support processes that balance both their security concerns and employee's wants. Therefore, this study explores the factors to consider when developing an organisation-wide BYOD strategy for adoption.

## 1.2 Background of the Study

The fast-paced modern life and an accelerated business process have led to the need for reliable and fast data access. As a result of the tremendous technological advances and the different means of communication, it is incomprehensible that people will not have access to continuous information and data. The mobile handheld devices, which recently became globally available, offers convenient

connections to the realm of data and information. New trends in the communication technology space (wireless technology) have also changed the way we approach and access the Internet and have thrust organisations to centralise their internal information systems. In this way, employees now have access to corporate data and information delivery that accelerates workflow and decision making (Saksida, 2008). The benefit of having a good knowledge of mobile devices and using them safely and efficiently lies in the competitive advantage it offers in both the business and science world. Contrastingly, there are questions about information security where organisations may choose to restrict unauthorised admission to information systems to prevent intruders from stealing and misusing their data, as this will increase business credibility, by signifying the importance of information security (Markelj *et al.*, 2013).

Mobile phones such as Android phones, iPhones, and iPads have become an essential part of humans' everyday lives. It is small and easy to move around with, but it is also capable of using powerful computational and storage capabilities. Unfortunately, these features also have their disadvantages. For example, a small mobile device can easily be stolen, especially in public places such as airports, cafes or libraries. Recently, aided by a tinier and more powerful mobile device, the amount of mobile device theft has heightened (Yang *et al.*, 2011). Almost every portable device has an in-built configuration to facilitate easier connection to the Internet, further enabling employees' mobile devices to connect to the corporate information system to transmit data. Some organisations deliberately have open network ports so that their personnel can work in virtual locations.

Mobile devices usually need to make provision for several numbers of security goals, ranging from integrity, secrecy, and availability (Souppaya *et al.*, 2013). For organisations to comply with these goals, organisational data must be protected against the many threats presented by these mobile devices. Mobile and computer networked services have opened new opportunities for organisations and employees to contribute to greater workforce satisfaction, increase productivity and improve competitiveness (Vodafone, 2013).

However, owing to the increasing numbers and types of mobile devices employees of an organisation can have access to, the risk of losing data or theft of corporate data is limited to data management issues (Vodafone, 2013). The process to safeguarding corporate data is important, especially when data from external sources and intellectual property are at risk.

### 1.3 Research Problem

Organisations are allowing their networks and data to be accessed on employees' portable devices such as tablets and smartphones (Trend-Micro, 2012). This rising trend creates a sensation known as consumerisation of IT in the office, where workforce personnel prefers to use their own portable devices as an alternative to those that will otherwise have been presented by their organisation (Garlati, 2011).

The inclination towards using a handheld mobile device may have occurred after the introduction of Apple's iPhone for the first time in 2007, the first handset designed to interface with multiple touches (Kim, 2011). Many advances have since been made in the smartphone industry, including the introduction of Google's Android operating system software. Hewlett Packard buying Palm and the cooperation between Microsoft and Nokia to release its Windows 7 phone while utilising Nokia's flagship hardware are also profound advances (Kim, 2011).

Consequently, from the time when the new generation of technology embedded in Apple's first iPhone, smartphone demand has been on the increase (Kim, 2011). As stated by Gartner (2018), 432 million units of smartphones were sold globally in the fourth quarter of 2016, this increased by 5% from 1.425 billion units in 2015 to reach 1.5 billion total units in 2016.

According to a survey conducted by Cisco among business leaders in South Africa to comprehend the attitudes and behaviours of staff towards the use of their personally owned mobile devices within the workplace, the results disclosed that despite the urgency for organisations to adopt BYOD policies, almost forty-six per cent of South African firms do not have a plan in place to cope with the use of portable devices for work-related activities (IT-Online, 2014). Also, different organisations do not fully understand the BYOD's model because of the challenges that come with it, such as weak policies and regulations on the BYOD model, insecurity of important data, and employee unawareness of the importance of the policy (Mwenemeru *et al.*, 2014).

It has been estimated that mobile usage in the working environment is expected to grow by ten per cent annually (Burt, 2011). Additionally, a study by International Data Corporation (IDC) on the consumerisation of IT revealed that forty per cent of IT tools used to access business applications belong to employees within the organisation (Mwenemeru *et al.*, 2014). As a result, IT divisions need to make a business decision on how to meet BYOD's challenge when planning their strategy on how data and information can be managed throughout the organisation. This strategy includes creating and implementing policies that regulate the level of access, ensuring the quality of service, and securing an organisation's data.

The objective of this research entails an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets within an organisation. The overall objective of the study is to document a set of factors that need to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of an organisational IT infrastructure.

## 1.4 Research Questions

The overall objective of this research is to document a set of factors that need to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of an organisation's IT infrastructure. The focus is on the corporate environment, to document/identify a set of factors to take into account when developing a BYOD strategy for adoption by the whole organisation. The research questions are organised around sections defined in the conceptual framework adopted by the research. The research questions are described as follows:

**Primary Question:** What factors should be taken into account before implementing a corporate BYOD strategy for mobile artefacts (smartphones and tablets) utilised by employees in relation to the following four selected classifications from the conceptual framework adopted by the study: (a) policy framework, (b) data security, (c) employee education, (d) mobile learning at work

### **Sub-Questions:**

- What factors are to be taken into account when developing a **policy** to be adopted for the satisfactory use and prohibited use of personal portable handheld devices?
- What factors should be reviewed to ensure an organisation's data is **secure** while allowing the use of individually owned devices by employees?
- What approach must be taken into account in order to raise **employee awareness** of safety benchmarks and pronouncements in the use of portable personal devices?
- What modality should be factored in when designing a **work learning experience** that satisfies the unique technical elements of portable devices?

## 1.5 Research Objectives

The research objectives are as follows:

- To determine the various factors to be taken into account when developing a **policy** for the acceptable and prohibited use of personally owned portable devices in the workplace.



- To determine relevant factors to be taken to guarantee an organisation's data is **secure** while consenting to the utilisation of individually owned portable electronic devices in the workplace.
- To ascertain the right approach to be taken into account in order to increase **employee awareness** of safety benchmarks and assertions when utilising personally owned portable devices in the workplace.
- To determine the right modality that can be incorporated when drafting **work learning experiences** that appeal to the unique technical elements of mobile artefacts in the workplace.

## 1.6 Significance of the Study

In this modern business world, employees use their mobile devices to accomplish their tasks in the workplace. Work emails and applications such as calendars, mail, and instant messengers are all being accessed by employees on their mobile devices.

On the other hand, employers need to be prepared on how to regulate the handling of employees' devices within their ecosystem. The ever-increasing influx of personal handheld devices has the potential to create an immense data security burden that most organisations are not prepared to handle. Not only have they not been shielding themselves, but most of them also do not even know how exposed they are.

The objective of this study entails an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets within an organisation. The overall objective of the study is to document a set of factors that need to be given priority consideration before corporate personnel are allowed the privilege of bringing personal computing devices into the confines of the organisational IT infrastructure. The study is vital in the sense that there is a lack of clarity on the parameters within which corporate personnel are allowed to use personal computing devices especially in the current global context where there are significant concerns regarding the integrity of organisational data in the light of IT security threats. The type of organisations in eThekweni Municipal Region, South Africa that would need to clearly define its parameters before allowing employees to use their mobile devices within its network also plays a role in this study's importance.

## 1.7 Research Methodology

According to Chinnathambi *et al.* (2013) and Kinash (2006), research methodology can be understood to be a systematic and organised technique to answer a particular research problem. It incorporates the

science of learning and conducting research (Kinash, 2006). It also involves the techniques, procedures or steps by which researchers go about their day-to-day activities in describing, analysing and predicting a phenomenon.

### **1.7.1 Research Approach**

For more complete and better interpretations of results and a greater understanding of the phenomena being studied, this study adopted qualitative research approach. The qualitative approach was selected because it will allow for the detailed investigation of the set of factors that IT managers should take into account when implementing strategies that accept and regulates the use of personally owned devices within the organisation.

### **1.7.2 Research Design**

To provide specific ideas, precise explanations and details of the phenomenon studied, a descriptive research design was used in this study. The descriptive research design was selected because of its approach to carefully observe, analyse and provide information on the set of factors that IT managers should take into account when devising a strategy that applies to the use of an individually owned portable device such as a smartphone and a tablet within organisations in eThekweni Municipal Region, South Africa.

### **1.7.3 Study Site and Target Population**

According to Patton (1990), there are no specified rules for measuring the sample size in qualitative research. He further explained that the qualitative sample size depends on the dimension the researcher is looking to explore. Considering the research approach for this study, fourteen (14) different respondents from different small to medium firms in eThekweni Municipal Region, South Africa were used in the collection of primary data and other required information.

The target population was an aggregation of the IT Manager/Administrator and CIO/CSO/CTO. The respondents to be interviewed had at least some influence on policy decisions regarding the device their company's employees could or could not use to access the network.

### **1.7.4 Sampling Method**

Since a qualitative research methodology formed the basis of this study, a non-probability sampling technique was employed for the selection of respondents. In non-probability sampling method, the selection of respondents that make up the sampling frame is often biased and non-random (Battaglia,

2008). A non-probability sampling in the form of the purposive sampling technique was selected as the sampling method accepted in this study for the selection of respondents. Purposive sampling was selected for this research as it allows for the selection of respondents in a non-random and deliberate manner (Battaglia, 2008). Respondents were, therefore, selected based on their executive decision-making positions held with the firms analysed in this study.

### **1.7.5 Data Collection Method**

An interview document was the instrument employed for obtaining data corpus from the respondents. The interviews were guided by a standardised open-ended interview to investigate the factors to consider when devising a BYOD strategy for adoption in an organisation in eThekweni Municipal Region, South-Africa. This approach would allow the researcher to draft a set of open-ended questions that participants can respond to sequentially (Marshall *et al.*, 2014). This interview method was adopted since it would help target the specific phenomenon the researcher is investigating. The objective is to gather as much correct information regarding the phenomenon being investigated without having to do a follow-up interview for missed or forgotten questions. During the interviews, data was collected from respondents using already prepared questions, interview protocol, and an audio recorder.

### **1.7.6 Data Analysis**

Data collected during the interviews was analysed using NVivo software and the type of analysis technique used was the thematic data analysis (Braun *et al.*, 2014). The thematic data analysis technique is a type of qualitative analytic method usually adopted to enable the researcher to gain insights and generate knowledge from a data set (Clarke *et al.*, 2013). The thematic data analysis technique was employed in this study to identify and analyse essential patterns and themes from the qualitative data obtained from the respondents.

## **1.8 Limitation of the Study**

The primary limitation of this study is that it was focused on BYOD for a precise organisation type, this allowed the study focus commonly on the factors involved in order to support an organisation's BYOD goal strategically. The study does not recommend implementing the model for an organisation's data networking facilities, but rather how to set up the organisation's data network to improve its security, which relates to the use of a privately-owned mobile device by its personnel.

## 1.9 Structure of Dissertation

The structure of the dissertation gives an overall summary of each chapter in this research study.

**Chapter 1:** This chapter starts with an introduction and background to the study. It also describes the research problem, research objectives and research questions that the study aims to answer. It further gave justification and significance for carrying out this research, including a brief description of the research methodology employed in the research.

**Chapter 2:** This chapter presents a comprehensive review of the literature on a BYOD strategy. Several definitions were given with the description of key concepts that made up the research study. The chapter also elaborates on various works of literature on a BYOD policy, BYOD and data security, BYOD and employee education, BYOD and mobile learning. It further included the conceptual framework that would go on to guide the empirical phase of the study, including the process with which the framework was validated.

**Chapter 3:** This chapter outlines the research methodology adopted in the study. It also presents the method of data collection, the data collection instrument, the sampled population, and the sampling method used in the study. The chapter also outlays the data analysis technique adopted in the dissertation.

**Chapter 4:** In this chapter, data obtained during the empirical phase was extensively analysed and discussed using the thematic analysis technique. In order to accurately present the research findings, a conceptual framework was used in tandem with the literature to properly address the objectives of this research study by identifying various factors that IT managers need to consider when implementing strategies for the use of personally owned mobile artefacts (smartphones and tablets) within an organisation.

**Chapter 5:** This chapter gives a summary of the key conclusions obtained during the analyses of data and discussions of findings in the fourth chapter. It also concludes by recommending areas in the study that require future research work.

## 1.10 Conclusion

The researcher has introduced the reader to an overview of the study, which talks about what an organisation needs to know before developing a BYOD strategy. A definition of the problem statement has been formulated, an overview of this branch of knowledge, concerning the groundwork of a BYOD approach for corporate organisations, has been presented. This chapter also discusses the research questions, research objectives, the problem statement and research limitations.

## CHAPTER 2: LITERATURE REVIEW

### 2.1 Introduction

This chapter begins by introducing the concept of BYOD and the general review on BYOD. It reviews different kinds of literature that explain the benefits and challenges of adopting a BYOD strategy. Similarly, this chapter also reviews the literature on BYOD adoption in the IT industry in South Africa, and additionally, policy framework and adoption in South Africa. The chapter also introduces the conceptual framework that would go on to guide the empirical phase of the study, including the process with which the framework was validated.

#### 2.1.1 Introduction to Bring Your Own Device

The concept of BYOD is regarded as an act or process, in which the managers of an organisation allows the use of personally owned mobile artefacts (tablets and smartphones) by its workforce personnel among other many devices for work commitments (Brandly, 2011). In accordance with an article titled: "*what is Bring Your Own Device (BYOD)*", it has been made known that the two main reasons for this BYOD occurrence includes the organisation's efforts to minimise the difficulties, the financial cost that comes with managing enterprise mobility, and employees' preference to make use of accessible devices rather than devices provided at work by their employers (Garlati, 2011). In a report by Trend Micro from 2011, Garlati (2011) noted that employees prefer to utilise their own devices at work since it is convenient, more comfortable to use as it empowers them to merge their work-related and personal information into a container.

From a global perspective, the adoption of BYOD in organisations has been quite rampant (Omwenga *et al.*, 2015). BYOD is an environment where employees have been noted to indicate that their employers allowed them the satisfaction of connecting their personally owned mobile artefacts (smartphones and tablets) to the enterprise network for work-related activities (Mwenemeru *et al.*, 2014). In the United Kingdom, the adoption of BYOD concept in the organisation dropped to thirty-seven per cent, in this same time, there was an increase in India to the tune of eighty per cent and ninety-two per cent in China (IT-Online, 2016). The increase of BYOD concept in these countries can be directly linked to the increase in opportunities of new IT infrastructure development; thus, this makes emerging economies an enabling environment to adapt to the modern policies and technologies presenting themselves as opportunities (IT-Online, 2016). In emerging economies, the tendency to accept the BYOD policy in the organisation is becoming more and more critical. For example, over sixty-five of organisations in South Africa are interested in having an official BYOD's policy, and almost a third (thirty per cent) do not know how to implement it (IT-Online, 2014). With the Cisco

Visual Networking Index Global Mobile Data Traffic forecasting that in 2019, there will be over 98 million smartphone devices in South Africa. Cisco believes that the nation is rapidly approaching almost a point where every network experience will be readily available for consumption via a mobile device (IT-Online, 2014). One of the key developments resulting from this mobile phone explosion is the growth of the organisation's BYOD (IT-Online, 2014). Also, according to a study from Cisco among business leaders in South Africa to understand the attitudes and behaviour of staff in relation to the use of personally owned mobile artefacts within an organisation's IT network, found that despite the emphasis on the urgency for organisations to adopt a BYOD policy - the fact that almost forty-four per cent of South African companies do not have a policy in effect despite the existence of the BYOD policy in the country remains a challenge going forward (IT-Online, 2014).

BYOD describes a distinctive prospect for progressive organisations to exploit this corporate control to their advantage. However, this trend leads to new challenges related to data protection, data access, employee awareness, and work learning experiences that demand organisations to re-assess their current security and management policy (Crook, 2013). Considerably, IT divisions drove technology, but IT revolution has altered the IT culture to allow consumers to receive the modern, cutting-edge technologies first, and they then take these devices to work (Brandly, 2011).

## **2.2 Theoretical Review on BYOD**

The account of the BYOD concept may be related to the enhanced and continuous advancement of Information and Communications Technology (ICT) integration on different electronic devices. Over the years, organisations such as Samsung and Apple have invested in the redesign of their mobile phones, among other electronic gadgets to meet their user's everyday demands (Chen *et al.*, 2011). The several features embedded in these devices allow employees to be more engrossed and active to handle office tasks using their personally owned mobile artefacts (smartphones and tablets) instead of devices provided by their organisation.

Also, this concept allows employees to transit between their business and personal work effortlessly smoothly; this works based on ordinary motivation (Trend-Micro, 2012). Over time, organisations will recognise that employees are actively committed to using their own mobile devices to carrying out their official duties, so they choose to continue the concept by permitting employees to come with their own devices to work (Mwenemeru *et al.*, 2014).

However, many organisations have not adopted the whole idea of BYOD because of the challenges that come with it. Some of these challenges range from employee unawareness of the importance of the

policy and lack of security of important data (Mwenemeru *et al.*, 2014). The BYOD revolution is only innovatory for IT divisions that choose to compete with an unknown number of devices penetrating the organisation's network every day. This complexity can be further driven by changes in the safety and conformity of those devices with established standards, even though such standards exist (Brandly, 2011). Employees often possess multiple devices and these devices hardly match any pre-conceived thoughts on the appearance of what a standard device might look like within the organisation.

Currently, the trend of BYOD has become more prevalent in recent years. An ISACA study shows that fifty-four per cent of employees out of the global workforce bring their device to work (Omwenga *et al.*, 2015). Employees enjoy the freedom that the BYOD model offers. Likewise, the balance sheets of the organisation look healthier for the little they spend on computational hardware. The ease of BYOD, however, is accompanied by a tremendous risk to data security, which can prove very costly for organisations as they are deprived of control over many of the hardware and the way it is used by employees (Brandly, 2011).

### **2.2.1 Benefits of Implementing a BYOD Strategy**

Some advantages can be achieved by adopting the BYOD model by the organisation. In general, employers and employees can both benefit in various ways. For example, companies that accept BYOD have allowed themselves to reduce the cost of expensive computing devices they would have to buy for their employees (Koeberl *et al.*, 2012). Employees can adequately maintain devices that they view as their own. Organisations can benefit from the latest technology usage. On the other hand, employees can also decide on which technology they should use for work instead of being limited to a company's device (Koeberl *et al.*, 2012). The BYOD concept can not only be about the device but also about the software section as well. Organisations with a consumerism attitude increase their risk-bearing as a result of the steps they have taken to address probable vulnerable areas instead of concealing their viewpoints (Crook, 2013). Additionally, organisations that allow employees to work with the most available technology tend to gain a more satisfied workforce as well as save the organisation a lot as benefits from cost savings (Crook, 2013). Besides, Singh (2012) argued that the company adopting BYOD's strategy could boast of a workforce that is more productive, collaborative-intensive and happier. Consequently, we can conclude that using personal devices in the workplace has a positive value from an employer perspective.

According to Fogarty (2010), an IPASS study, conducted among 1,100 mobile workers, showed that staff with dual functional devices recorded a further 24 hours a year than those who did not. Employees that are permitted to using their own handheld devices will likely enjoy high mobility, job satisfaction, efficiency, and productivity improvements. This value is translated in favour of the enterprise (Fogarty,

2010). According to a survey of small IT contractors, most of those surveyed said that spending had decreased or remained the same since the introduction of BYOD in their respective organisation (Trend-Micro, 2012). This survey confirms the theory that organisations are reducing their IT capital expenditure (because employees are allowed to bring their own devices), thereby reducing IT infrastructure maintenance costs while also increasing employee productivity (Harris, 2012).

From an enterprise perspective, BOYD consumption and usage can be seen as a competing factor for organisations, making it essential to their business objectives. Cisco stated in its Connected World Technology Report that seven out of ten youthful job seekers admit that the absence of virtual remote access to work terminals can affect their decisions about jobs such as him/her resigning from a job immediately or entirely declining a job offer (Marshak, 2006). It is sensible to infer that users will have the same expectation about their portable device(s); i.e., an organisation should allow its employees connect to the virtual machine resources irrespective of the source of the device, either dispensed by the organisation or employee-owned. According to Trend Micro's IT Executive and CEO Survey, BYOD is seen as advantageous for engaging any active personnel with a significant increase in productivity, innovation, and maintaining a balance between work and private life (Trend-Micro, 2012).

Eight-six per cent of hospitals surveyed in Sunnyvale, California, were reported to have adopted strategies that support the use of employees' personally owned mobile artefacts for work activities (Networks, 2012). Even seven per cent of the hospitals, out of the eighty-six per cent surveyed, enabled complete access to corporate networks for applications such as Electronic Medical Records (EMRs) which is expected to snowball as a result of the pressure from its clinical employees on IT department to open access to its network(s). Another health-related study conducted by IDC, which oversees insights in 50 hospitals in both European countries and the United States of America (USA) in November 2011, showed the same statistics (Crook, 2013).

In addition to employee satisfaction and business productivity often considered a significant advantage for organisations that have adopted a BYOD strategy. The benefits outside the ones reported include improved cooperation and adaptability, increased access to mobile device resources, lower costs on retrieving and maintaining devices, decreased responsibility for maintaining the life of devices and unification of tools and infrastructure across the different IT disciplines (Edelheit *et al.*, 2012). Cummins *et al.* (2012) pointed out that modern personalised devices such as tablets, laptops, and smartphones offer uncompromised convenience in computing power. Portability provides communication on demand that allows employees to solve time-sensitive challenges from a remote distance, preventing traffic lags and inadequate access to software resources. In addition to providing remote access to these devices, the more productivity-driven a remote work is, the flexible the demand



for employees to arrive at stringent working hours or working in a controlled professional environment. This modification plays a role in attracting staff with persistent family responsibilities or disabled members of a community (Cummins *et al.*, 2012).

Sen (2012) conducted a survey on the use of consumption of IT benefits, purpose and problems for the New Zealand Corporate, from the outcome of the survey, it was noted that some benefits of the adoption of BYOD, consist of, but not limited to an accelerated business productivity and growth in the organisation, arising from personnel introducing new technology devices, personnel work output through cost, and trust to their organisation (Sen, 2012). As already noted, many advantages can be achieved by taking the BYOD concept into the organisation. Sen's research serves as the basis for the study's primary purpose, to highlight the factors that IT managers should consider when implementing a BYOD's model in a South African organisation that is based on the benefit of BYOD's strategy.

### **2.2.2 Challenges of Adopting a BYOD Strategy**

BYOD's risks are classified into two broader groups. The first risk is the fact that the organisation's data can be stored and shared through devices owned by employees whom the employer cannot control or manage. Losing control may contradict the government's growing regulatory requirements, which require organisations to safeguard the privacy and safety of sensitive personal and financial data. Similarly, it can pose a risk to protect the confidentiality of the business, assets, or company information (Markelj *et al.*, 2015). The second risk refers to the impact that BYOD policy can have on employee behaviour. The second risk directly highlights some rules that provide employees with information on how to use their device correctly when connecting to a corporate network, while maintaining the best ethical principles to implement while ensuring the well-being of an organisation's data and network systems without compromising employees' incentives and productivity (Wittman, 2011).

The challenges facing BYOD's strategy have been addressed through the use of a new type of mobile app called Mobile Device Management (MDM), which gives employers the tools to control the dual-use devices of their employees (Koeberl *et al.*, 2012). Sadly, this tool can only mitigate these challenges and not completely eradicate them (Koeberl *et al.*, 2012). Therefore, employers need to modify or create new policies and operational procedures to incorporate new employee contracts or expand and create tremendous insight into these issues to promote an all-around work learning practice that ultimately supports a BYOD enabled work ecosystem (Wittman, 2011). The likelihood of companies that embrace the BYOD policy that let business data to be stored on private mobile devices owned by employees is high. This causes data-related challenges for companies, mainly those in highly-managed environments such as healthcare, financial services, and other organisations that are responsible for managing sensitive personal information (A. Harris *et al.*, 2014). Best practices such as programmed locking;

password protection and encryption, including budget allocation on funding security awareness and educating users, can solve many problems of portable mobile access (A. Harris *et al.*, 2014). Other possible constraints are that employees use devices they own and thus can alter their expectations about what equipment to use correctly, this change may lead to conflicts with the company's policies. This means that the personal ethics/morals of some employees who are active social networkers can diverge from other non-social networking employees on crucial issues (Kellogg *et al.*, 2014). In a National Business Ethics Survey (NBES) conducted in 2011, the Ethics Centre detailed that staff who are active on social networks may be prone to believe that some questionable behaviours could be acceptable (Kellogg *et al.*, 2014).

### **2.2.3 Telecommunications Industry in South Africa**

In 2010, the International Telecommunication Union (ITU) proclaimed that South Africa had a reasonably low amount of fixed-line telecommunication service consumed by around 4.2 million people. The landline technology is controlled by Telkom which also list on the Johannesburg Stock Exchange (JSE) with the bulk of its ownership controlled by the country's Department of Communications. Telkom's exclusivity with fixed-line services terminated in 2006 after the introduction of Neotel, who offers the same service. Neotel, which is primarily owned by Tata Communications in India, provides both voice and data services to approximately nine million subscribers in South Africa (SaInfo, 2013).

The use of mobile phones in South Africa expanded from sixteen per cent of adults in 2000 to seventy-seven per cent in 2010 (SaInfo, 2013). In 2012, more than 29 million South Africans used portable phones as compared to television (27 million), radio with 28 million or personal computer (PC) with 6 million. Fewer than 5 million inhabitants use fixed-line telephones (SaInfo, 2013).

The increasing use of mobile phones and smartphones has led to an increase in Internet usage. At the end of 2011, there were 8.5 million users, up from 6.8 million in 2010. It was predicted that by the end of 2018, the 35 million user limit will be broken (World-Wide-Worx, 2012).

### **2.2.4 BYOD Adoption within the IT Industry in South-Africa**

The South African IT market, comprising of both the software and hardware businesses, is considered one of the most leading and modern sectors within the continent. It is among the world's leaders in areas such as e-mobile applications, prepaid payments technology, revenue governance, fraud deterrence and set-top boxes manufacture with some products designed for export markets (SaInfo, 2013). South Africa's IT industry was assessed to be worth 77.1 billion Rands in 2011 and has grown nine per cent

annually to reach 116 billion Rands in 2016 (ICT-Policy-Review, 2013). It was reported that there were about 2000 information technology organisations at the end of March 2012 (Mictseta, 2012). The IT business niche is the most progressive (fifty-two per cent) followed by hardware (thirty-two per cent) respectively and software packages at nineteen per cent of the total IT market. Most hardware sub-market income is driven by networking and storage services, while Cloud Computing is reputed to lead further development in the IT services market.

For IT services, the allowance of this market hinges on large government programs. There are confusions between IT services and telecoms services as a result of a high rate of mobility. In South Africa, smartphones act as a replacement for PCs as a chosen method of computing and gaining access to the Internet. It was projected that by the end of 2019, consignments of smartphones would surpass 4.5 billion (ICT-Policy-Review, 2013). Besides, the smartphone computational power is expected to grow and will shortly run at 2.9 GHz processing power.

With the accelerated acceptance of mobile devices in South Africa, organisations have been trapped in a back-foot with the fastest growing trends in the local IT sector. The per centage of personnel who connect to their work network is broad, and this is a surprise for many IT divisions (Eugene, 2014). According to Andy Openshaw, Chief Executive Officer at Nashua Communications who reported that *"organisations are not geared up for the BYOD; as a result, they are missing out on the substantial rewards associated with this move for mobility. BYOD has been proven to increase workforce productivity and effectively connect applications, resources, and users, regardless of device and location."* (Mansfield-Devine, 2012).

A pilot project conducted in Eastern Cape, South Africa reported that using 3G enabled mobile phones helped doctors and nurses make a corrective diagnosis, and determine the right treatment which translated into the reduction of patients' death rate (ICT-Policy-Review, 2013). Doctors and nurses can also provide patients with the latest information on their welfare and medicinal challenges, also allowing these clinical workers to upgrade their knowledge of clinical procedures and share details with their co-workers. So, it can be assumed that organisations adopt BYOD's concepts to be able to operate with technology tools from their staff to provide excellent services and control the amounts invested in IT infrastructure for workplace development.

## 2.3 Policy Framework and BYOD

It can be noted that the concept of BYOD is not solely based on transferring device ownership to employees; it is a difficult concept that has hidden consequences in need of a pre-defined strategy. As a result, many factors are to be addressed by organisations before adopting the concept of BYOD.

Moschella (2005) indicated that various vital components are to be considered for the adoption of the BYOD concept in an organisation. Some of these essential components include the formulation of a policy framework that encompasses the type of mobile device to be used, specification of the operating system to be used on devices.

The development of a BYOD policy framework is the starting topic for adopting the BYOD strategy for the whole organisation. The policy should consider issues that explain the difference between processes and procedures (Wittman, 2011). In the BYOD environment, the IT policy must adopt specificities compared to traditional policies that neglect the personal device usage and data network security challenges that the IT division still controls.

Additionally, a BYOD policy for IT consumption should be established in cooperation with an organisation's workforce. In a dialogue with Frank Andrus, technology director at Bradford, a BYOD policy development channel must include direct users, because the central system should have high visibility of the devices used in the organisation, and also the usage of these devices (Mansfield-Devine, 2012). At the same time, IT division should educate employees about the dangers and restrictions on the use of personally owned mobile artefacts (smartphones and tablets) at work (requiring training, collaborative work between IT division and users) (Mansfield-Devine, 2012).

Andrus underlined the 9-step process for the development of IT policies that support the use of portable devices in the workplace (Mansfield-Devine, 2012). He advised that before an organisation participates in BYOD development, the governance team should determine who could lead the unit through the stage of evaluation, development, and implementation. The recommended steps are:

1. Decide which portable mobile devices an organisation will provide consent to supporting.
2. Decide on the types of mobile operating systems that an organisation will accept.
3. Decide on what type of mobile applications would be accepted, and the type of applications will be rejected.
4. Decide on which category of employees will use these devices
5. Decide on the network connections that should be delegated to which employee based on what, when, who, and where.

6. Notify employees before they are permitted to use their devices on the organisation's network.
7. Record and monitor both unauthenticated and authenticated users.
8. Control access to an organisation's network resources based on the suitable level and understanding of the risks involved.
9. Make sure there is a continuous consideration in assessing vulnerability and remediation.

### **2.3.1 Factors to be considered in the development of the BYOD policy framework**

For this section, the framework offered by (Wittman, 2011) in his textbook "*Management of Information Security, 2nd edition. (2007)*" was reviewed. The guideline includes precisely seven sections that give mindful; details, aimed at informing all participants in the organisation about the use of the specific issue. The section took into account ways to manage: statement of purpose, authorised use, prohibited use, systems management, policy violations, policy review, and limitations of liability (Green, 2007).

#### **2.3.1.1 Statement of Purpose**

This part of the framework describes safety standards for portable devices. Mobile devices must be protected to safeguard the organisation's data assets, and also prevent the spread of malicious programs, such as viruses (such as Trojan horses) on the computing IT assets of the organisation, and limit unauthorised access to the organisational network (Green, 2007). This policy is applied and imposed by senior IT administrators, IT managers, and administrators (Mansfield-Devine, 2012).

#### **2.3.1.2 Authorised Use**

In this segment, authorised users and technological use are detailed. An example describes an employee whose organisation has purchased a mobile device for and has been only authorised to use them for business-related purposes only (Mansfield-Devine, 2012). Also, following the principle of existing organisation privacy practices, employees are reminded that they do not have privacy expectations when using an organisation's portable devices (Harris, 2012).

#### **2.3.1.3 Prohibited Use**

In this part, users are informed about what they can and cannot use the technology and mobile devices within an organisation. An example describes prohibiting the use of mobile artefacts by personnel for activities that are not associated with the organisation's business activities (Green, 2007). Other examples may include web surfing for non-business activities such as making or receiving personal phone calls, store personalised music on the device, email checking, personal files transfer or storage (Wittman, 2011). Employees are restricted from using an organisations' portable device to deal with any unlawful activities, offensive or harassment of any kind that will tarnish the reputation of the

organisation (Harris, 2012). Employees are also restricted from uploading any software applications on the device, as this has to be approved by the IT division, if necessary (Wittman, 2011).

#### **2.3.1.4 Device System Management**

In this part, policy authors emphasise the users' association with the device system management (Wittman, 2011). For portable devices, this section can be widespread. A device system management layer can define measures for workers using portable devices to approve that the following requirements are met when using a portable device in an organisation, as well as any applications or data stored on these devices:

- Power-on verification: Users should be obligated to enter a secret token upon powering on the device to reduce threat if a device is misplaced or stolen.
- File/Folder encryption: Users should make sure that individual files and folders that include organisational data are encoded.
- Antivirus software: Users should make sure that the antivirus software set up on the portable device is the latest and running continuously.
- Lost/Stolen/Missing device: Users should promptly report a lost/stolen/missing portable device to the IT division.
- Protected wireless transmission: Users must, on no occasion, transmit any data over an insecure wireless network. The Virtual Private Network (VPN) client must be configured on the device, and the wireless network must be encrypted.
- Firewalls: IT division should make sure the installed firewall client on the employee's device is running and up-to-date.
- Passwords: IT division should advise employees on how to create robust passwords to encrypt their portable devices.

#### **2.3.1.5 Violations of Policy**

For this section, users are notified of proper consequences if they breach the policy and how to report abuse by others (Wittman, 2011). An appropriate example here is telling the employee that there are punishments involved in contravening this policy. In the first offence, the employee will be given a written caution from his manager about the occurrence. For the second attempt, the employee will be suspended for a week short of pay as well as other written warnings. For the third violation, employee's employment in the organisation could be ended (Green, 2007). Management reserves the right to impose penalties on specific abuse of policy (Green, 2007). All employees are strongly urged to report any alleged violations of these policies. These reports may be posted secretly using the internal watchdog website of the organisation (Harris, 2012). No personally identifiable evidence was required on this page and was not saved in the server log (Harris, 2012).

### **2.3.1.6 Policy Review and Modification**

In this context, users are informed of what way and as at when a BYOD policy will be revised. This policy can be reviewed every year or twice in a year, and all updates are issued on a precise date. The policy will be studied by a commission appointed by the head of the Information Security Unit of the organisation (Mansfield-Devine, 2012). The committee will be appointed on a particular date and must be publicised on the organisation's circular (Wittman, 2011). Additionally, committee contact information should be published so that employees can offer criticism that they think may guide the selected committee in changing or reviewing the policy (Wittman, 2011).

### **2.3.1.7 Limitations of Liability**

For this context, the organisation strives to defend itself legally by showing a specific set of liabilities if the rule is not respected (Harris, 2012). This guarantees that the organisation is not accountable if the employee intentionally disrupts this policy leading to any criminal or conviction penalties (Wittman, 2011). The organisation will not provide any protection or assistance to its staff if they are accused of a crime while violating these rules. The organisation refutes any liability or delinquency to intentional employees who violate this policy (Green, 2007).

## **2.4 Data Security and BYOD**

Using personal devices pose a risk to data security in both a user's organisation and user's data. Mobility's competitive benefit can be intact if employee personally owned artefacts (smartphones and tablets) are not sufficiently shielded from security threats to these devices. According to Markelj *et al.* (2015), IT divisions have acknowledged information security as one of their biggest apprehensions regarding the expansion of mobility. Portable devices are targeted at multi-level threats that can work alongside each other; therefore, the tag blended threats (Markelj *et al.*, 2013). Blended threats cause harm to users and organisations. The main threat stems from the possibility for theft or loss of portable devices. In cases where users have stored vital and personal information on their devices, but are not trained for simple protection, such as verification, the user will put personal data and organisation data in jeopardy (Markelj *et al.*, 2013). Indirect threats can be more substantial because it is unpredictable. For example, if a portable mobile device is connected to an organisation's network, as well as a public network, it can open a non-secure route to an organisation's primary information system that constitutes as security breaches (Markelj *et al.*, 2013). Mobile devices can become a portal to the raw information of the organisation unless appropriate precaution is taken.

### **2.4.1 Factors to ensure that Data is secured in a BYOD Culture**

Appropriate data protection in BYOD environment calls for a management system, access control of the information procedures not only to the user but also the sort of device is trying to access the network and where they come from (Markelj *et al.*, 2013). Suppliers also fully work out solutions for MDM entities and include some of the protection outlined above to protect data into their MDM software (Burt, 2011).

There are six factors acknowledged by this study that the IT division may consider in ensuring that organisational data is protected in a BYOD environment. These factors are discussed below:

#### **2.4.1.1 Segregate the Data**

IT division must plan for an organisation's data to be separated from a user's private data. According to (Wittman, 2011), this can protect an organisation from wasting energy in the event of litigation and compliance-related audits. One way to enable this is to provide storage space and communicate to users the processes for backing up their work-related data in this space and keeping their data out (Harris, 2012).

#### **2.4.1.2 Require Users to Register their Device**

An organisation's network registration process for connecting mobile devices may give the IT division the ability to track users' mobile devices (Markelj *et al.*, 2013). This process may also be a training mode towards the appropriate and inappropriate use of mobile within an organisation's network, including setting up privacy settings and data backups.

#### **2.4.1.3 Allow Remote Access to Personnel Mobile Artefacts**

If a portable device is misplaced or stolen, this precaution will permit the IT division to delete all data corpus from the mobile device by reducing the possibility of losing sensitive or personal data.

#### **2.4.1.4 Implement Data Encryption**

The encryption program is utilised to encrypt only part of the data corpus on a mobile device or the entire information system. Encryption is used to protect data or information from unauthorised access, and only those with access codes can access such data or information.

#### **2.4.1.5 Use Strong Passwords**

Strong passwords are to be requested from users trying to access an organisation's resource. The use of a strong password combination is requested for during mobile device registration on an organisation's network (Emery, 2012). This simple authentication procedure proves to be an adequate safeguard



against limiting unknown access to an organisation's resource such as wireless network, and information system.

#### **2.4.1.6 Install and use a Virtual Private Network Solution**

A VPN works on the principle of creating a private channel between two devices. Majority of the VPNs creates an established link between a VPN software on a mobile device and the VPN server located within an organisation (Emery, 2012). The link between the device and information system needs to be verified as well as the identity of the user before granting remote access.

### **2.5 Employee Education and BYOD**

Following the acceptance of individually-owned mobile devices on an enterprise network, there precedes the need for the IT division to train staff to help protect both staff and organisation data from attacks (Markelj *et al.*, 2015). By changing the template from a standardised platform of organisation structure and devices towards the BYOD paradigm, there are now different mobile device platforms that expose an organisation's assets and data for additional threats (Thomson, 2012). Thomson (2012) also reported that the BYOD operation is predictable and that the earlier organisations tackle the encounters and issues of BYOD, the better it improves itself in the future for the rewards. This factor is indicative of a changing paradigm from a technology-focused to a user-focused perspective on safety since the criteria for security across various devices are erratic.

#### **2.5.1 Factors to Address Employee Education in a BYOD Culture**

In this context, employee education and training, and employee awareness and motivation strategies are factors to be considered for development concerning employee's usage of personally handheld mobile devices.

##### **2.5.1.1 Employee Awareness**

Concerning the social unreliability factor, Albrechtsen (2007) contends that the key problem is the lack of user motivation and user knowledge about information protection. Albrechtsen (2007), in his study, states that corporate personnel frequently fail to comply with other safety and security requirements and guidelines and go on to craft other work duties over security. Research results from Post *et al.* (2007) also found that employees are becoming aware of the extremely rigid safety practices put in place by the IT division, which can be interpreted as barriers, making these employees bypass these practices to maintain their productivity level. These conclusions highlight the fact that users have a bad record of adhering to simple security procedures (Stanton *et al.*, 2005).

Herath *et al.* (2009) consider that incentives help to improve user's security-related behaviour. To confirm these motives, Siponen *et al.* (2010) provided the basics concepts and methods to encourage users to oblige to safety standards through security information programs. Siponen talks on how it is important for users to feel more intrinsically motivated to adhere and commit to security procedures and policies. i.e., the role of human factors is critical to the success of a BYOD security initiative. Therefore, the behavioural theory that Siponen *et al.* (2010) emphasises on is termed induced theory of incentives. This theory relates to consumer choice, which is their freedom to make personal choices regarding their behaviour. They must prove the correctness of their actions for fundamental reasons such as their ambitions, instead of external incentives in forms of financial gain. Creating an internal motivation to adhere to safety procedures is well-defined as internalisation, which pushes long-term involvement (Chen *et al.*, 2011).

Siponen *et al.* (2010) argued that users need probable reasoning and sensible display of information to increase their awareness of security procedures. Additionally, Stewart *et al.* (2012) reported that consumer-related security concerns are thought to be triggered by the absence of information and facts available to them. BYOD security policies that are designed with the user in mind will allow for intrinsic motivation to be realised through other principles such as user's ethics and moral, and their feeling of security and well-being (Siponen *et al.*, 2010). Albrechtsen *et al.* (2010) also believed that customer motivation is a key component for a security awareness program and has indicated that security concepts ought to be easy, speedy and easy to grasp.

### **2.5.1.2 Employee Motivation**

Some organisations are focusing on setting up security policies for personal mobile devices' use in the company but ignoring the motivation of encouraging consumers to stick to the recommended procedures and safety policies. While education and teaching will increase mindfulness of BYOD's security issues, unmotivated users will most likely not follow these safety guidelines.

In BYOD, device liability is shifted to users where they are anticipated to control the safety of their devices. It is, therefore, important for employees to play an active role in the advancement of the training and educative program. This will aid users to feel more linked to security policies and promote security associated obligation.

To inspire users to accept BYOD security guidelines, Siponen *et al.* (2010) have revealed some of the principles and methods proposed to motivate users. These methods comprise, but are not limited to:

**Morals and Ethics:** This technique is built on the concept that if users understand the ethical and moral extents of BYOD practice and the adverse consequences of violating their device, they are more likely to follow the instructions (Siponen *et al.*, 2010).

**Well-being:** The purpose of this methodology is to create users' awareness of the safety repercussions and how they can affect the well-being of other consumers and the organisation (Siponen *et al.*, 2010). Penalties may be moral or immoral, such as financial loss or breach of a work contract. Users who are alert of the costs of mobile security violations for their well-being and the well-being of the organisation support incentives that meet the terms of BYOD's guidelines and policies (Siponen *et al.*, 2010).

**Feeling of security:** This is to fulfil the needs and desires of the users to make them feel safe and protected. Siponen *et al.* (2010) conclude that society wants to uphold a sense of security in accordance with safety procedures. A sense of security can be created to permit users to recognise the significances of user privacy and direct threats, emphasizing privacy breaches and access to their personal information without permission. It also provides organisations with the need to educate mobile device users about how to protect their device by using secure passwords to deny unauthorised access to sensitive information.

### **2.5.1.3 Education and Training**

Albrechtsen *et al.* (2010) argued that users' involvement, discussion and mutual consideration in training and educative programs had demonstrated positive changes in the understanding of short-term security and performance. The “*intervention program*”, which reflects the findings aimed at enhancing customer perceptions of information security, found that the most efficient and effective program was a workshop intended to influence the procedures (Albrechtsen *et al.*, 2010). Beaulieu *et al.* (2009) stated that as a result of the small attention period of the users, training programs are to be dispersed briefly and efficiently. This further explains why the regularity and period of these workshops need to be shortened while still being useful in providing information about the policy. It has also been established that the impact of the workshops on safety awareness and behaviour continued for a year after educational and training programs, but the understanding of information security concerns has decreased (Goucher, 2009). Kim (2010) found in his research that a computer-driven safety training program as compared to a work-based seminar is much more effectual in retaining information. Users from the instructor-based programs have a significantly decreased result when they take the 60-day test. The knowledge that is transferred by instructor-based training is faster than computer-based training but does not necessarily mean that the information will be retained. Also, Kim (2010), found that, after 90 days, users, both from a computer and instructor-based training, did not differ significantly in relation

to knowledge retention. They have returned to their previous level of subject knowledge before these training programs.

A study of an intermediation program, conducted by Albrechtsen *et al.* (2010) said workshops which were not encouraging or engaging were unlikely to lead to transformations in behaviour; supporting Siponen *et al.* (2010) requests for internal motivation in training process through the enthusiasm that can be derived from educational programs and educators. Hagen *et al.* (2011) also specified that a fun factor could be further incorporated in their BYOD security awareness program because it is a valuable feature that makes users curious and excited.

The BYOD security concern, as determined by Peraković *et al.* (2012), will need training and educational method to raise knowledge of the threats that are positively aided by negligence or ignorance of the user. If a user is well-versed in training that his/her identification may be stolen when operating a mobile device, he/she will be more concerned about its safety.

Moreover, it should promote awareness of the security vulnerabilities of mobile devices, especially in the context of a threat to an information system application, and network security, as customers tend to believe that there is no need to download security software on their devices (Theoharidou *et al.*, 2012). Workshops personalised to present these portable device liabilities must aim to be collaborative and raise enthusiasm within employees while also being associated with the employee's work activities and responsibilities. To evade hampering the perceptions of education and training by users, teaching and training programs should be short-spanned and brief, yet efficient and effective in communicating information to the users.

Workshops and training programs, led by experienced teachers, have been found to be very effective when it comes to the communication of information to users, although computer training programs were more operative in data retention (Albrechtsen *et al.*, 2010, Kim, 2010). In order for teaching to have a long-lasting impact, organisations have to provide their staff with computer-based training materials and organise workshops that are fundamental to confirming BYOD's security awareness. Providing these planned workshops and training programs is endorsed as part of the hiring process in an organisation. It ought to also be proposed at consistent times all through the entire calendar year if the employee requests that their device is to be permitted for use in the network (Harris, 2012). These workshops and training programs should take place almost between every 90-120 days, the time when users are predicted to return to old security knowledge and habits (Alzahrani *et al.*, 2012).

## 2.6 Mobile Learning in Organisations

Mobile communication, including wireless communication, alongside smart mobile devices, are enabling remote connection to an organisation's information systems that are not restricted by either place or time. Additionally, these devices, which enable communication among employer and employee both inside and outside the organisation, have the perspective to modify the notion of the workplace (Akour, 2009).

Learning requirements via mobile devices have experienced a huge shift due to the proliferation of mobile and information tools (Akour, 2009). The influence of mobile communications has just started to be valued, and new frontiers are being explored and studied. Learning via mobile tools is an encouraging area for aiding organisations to meet the hassles of the innovative digital net generation, enabling learning for employees in numerous ways free from the limitations of place and schedules, and increasing the organisational system's outreach to employees. Mobile learning facilitates universal access to information, computing, and learning.

According to Pimmer *et al.* (2010), mobile learning seems to be a fast-rising sensation. In the field of workplace learning and work-based education, mobile technology creates a great deal of interest. However, there is surprisingly little literature on how portable devices can be used successfully, to learn and to develop employee for workplace tasks - except for early practical studies and theoretical and conceptual discussions (Pimmer *et al.*, 2010). In the context of this study, mobile learning in the workplace is the idea of an incomplete and growing field of practice and research.

Like any technology invention, portable mobile artefacts have the potential to revolutionise and improve modern educational practices. However, owing to the use of technology so far, the inconsistencies seem to be true (Pachler *et al.*, 2011). It has been argued that new technologies be mainly used to strengthen conventional, instructional and instructor-centred pedagogical approaches (Attwell *et al.*, 2009).

Mobile learning has primarily been applied and inspected in schools and institutions of Higher Education. Organisations tend to be more cautious about set up mobile technologies for learning (Härtel *et al.*, 2007). Pasanen (2003) in his book "*Mobile Learning*" addressed corporate mobile learning, where he termed it as the process of utilising the flexibility of portable mobile artefacts (smartphones and tablets) for the development and construction of learning material, for learning communication and for the supervision of learning. Pasanen established the significance of incorporation of mobile learning into the business information infrastructure and the intentional importance of mobile solutions. Mobile learning reassures innovation and proposes new business prospects. Moreover, Pasanen recognises

further profits from various perspectives, for example, actual learning material collection or enhanced customer service (Pasanen, 2003).

Non-scientific contributions from the field of commercial and industrial training show that businesses can take advantage of this form of technology that is difficult to understand. According to Weekes (2008), who collected data from a bank which disseminated audio messages to workers established that the response from the involved managers was 100 per cent positive. Another major commercial institution once provided training to their workers using Blackberry mobile phone. The results involved timely completion, and a higher completion rate of over twelve per cent paralleled to the control group within a two-month review (Swanson, 2008).

Mobile learning is similarly being implemented in the ICT sector. A complicated engineering situation was presented by the French Research Institute (David *et al.*, 2007) in the capacity of a mobile educational platform that gives engineers the chance to study minor contextualised and adopted learning arrangements while repairing or constructing manufacturing factories. This content is displayed on wearable devices like see-through goggles with an integrated screen which is served via a wireless local area network (WLAN) and Radio Frequency Identification (RFID) technology. If an engineer is in trouble, he or she can interact with an expert via chat or email which habitually includes machine references. The objective of the activity, apart from machine repairs, is to integrate key tasks and repair ethics. However, this situation has not yet been tested in other companies (Pimmer *et al.*, 2010). In the third case, a multinational technology company and a large consulting firm provided little personal information for selected staff. This profile is based on Human Resource (HR) data and is complemented by staff rendering of their qualifications, experiences, and interests. If the content is correct, the apprentice is alerted immediately by e-mail or by Short Messaging Service (SMS). As a result of immense technological necessities, only a few employees have the opportunity to download the content on their mobile device (Von Koschembahr *et al.*, 2005).

In an on-the-job education venture, a portable diary and feedback application were created for trainees who work temporarily in an organisation. These trainees solved their everyday questions about events and thoughts on their mobile devices. Also, they could record their considerations and augment their response with images, videos, and sound recorded with a camera device. An assessment of twenty-two (22) candidates focuses on the accessibility of the product. The use of the device has not undergone appraisal so far (Pirttiahho *et al.*, 2007).

Another example that demonstrates the creation and sharing of learning materials by apprentices involves clinical staff in an intensive care unit, who filmed their handling of technical equipment with

a video camera. These sequences were made available to co-workers who observed them on the mobile device instantly on-site via RFID technology. A scientific assessment shows that these practices increase informal peer-to-peer learning (Brandt *et al.*, 2004). Regardless of popular mobile gadgets with the ability of cameras and online video platforms, the practice of creating and sharing this video has not come into use until now in business.

Corporate learning, in general, is more focused on the content than based on social interaction (Traxler, 2007). It remains to be seen whether the emphasis will be shifting from mobile devices, whose communication capacity is designed to be very important for mobile learning developments (Sharples *et al.*, 2005).

### **Motivation for Mobile Learning in Organisations**

The nature of the organisation and how they undertake work has been transformed considerably over the last few decades. There is a great deal to handle higher unemployment, technological change, and more workforce mobility (Pimmer *et al.*, 2010). For example, mobile technology is changing the nature of the work, and the stability between teaching and support for efficiency (Traxler, 2007). This change, instigated by mobile phones, can only lead to better efficiency and control, but also weakens the boundaries of home and work (Traxler, 2007). This trend impacts on workplace learning and also impacts competence development, it is understood that smaller companies do not have adequate resources to sufficiently support the development of its employees' capabilities, hence, they can benefit from the virtual collaboration that leads to learning and knowledge transfer throughout the organisation's environment (Mazzoni *et al.*, 2009).

In recent decades, job skills have grown considerably. On the one hand, some of the jobs that have a short induction time has decreased. Contrastingly, an increasing number of employers have shown that their work requires constant learning, and employees find that they are helping other co-workers to get more collaborative at work to learn something new. This evidence proposes that an important driver for learning is the workplace itself (Felstead *et al.*, 2009). According to Pimmer *et al.* (2010), learning in the context of work is deemed necessary in today's learning society. However, it is known that these potentials are not met merely by recognising that learning is happening at the workplace: both the practice and teaching of learning in the workplace call for better understanding and development (Pimmer *et al.*, 2010). It should be understood that the principal objectives of many organisations are not to provide a learning platform but provide services and products focused on profits. Learning contributes significantly to this, but its value can be neglected because it is challenging to isolate it from everyday work tasks (Pimmer *et al.*, 2010).

It has been alleged that skills such as the ability to solve problems and autonomy cannot be sufficiently trained for from the outside. They must be created by self-direction in the suitable circumstances of learning (Hardwig, 2006). Staff should not learn "*just-in-case*" but in their work environment, through continuing variations in their organisation (Loroff, 2006). It is on this convincing notion that training personnel only in a classroom setting is becoming progressively tricky and unsuccessful (Hardwig, 2006, Loroff, 2006). However, classroom learning should not affect other forms of training. Instead, they can point to a new way of learning, which can advance the transformation of conventional classroom training into work routines (Bigalk *et al.*, 2006).

Mobile learning can also meet these difficulties of a diverse corporate scholastic landscape. Employees are entitled to access information independently in informal situations without access to an immobile IT infrastructure. Mobile devices can promote work activity learning: theoretically, it is promising to combine training and practice, and to access theories and information in the context it will be implemented - in the workflow (Attwell *et al.*, 2009). Thanks to focussing on cost savings, efficiency and savings in the short term (Kukulska-Hulme *et al.*, 2005), some companies may try to increase their throughput by "*just-in-time*" learning with mobile devices. The information can be retrieved when needed (Kukulska-Hulme *et al.*, 2005). Sharing photos and videos to resolve issues quickly can lead to a better direction. The mobile device may encourage the process of learning and reflection and purpose of the project for training in the workplace (Pirttiahho *et al.*, 2007). Additionally, they may seek to improve the transfer of learning, moving from face-to-face training into embedding these learnings as part of work routines.

### **2.6.1 Factors Involved in Designing Learning Experiences**

In determining factors to consider when organising learning experience in the framework of mobile artefacts in the workplace, the emphasis is on how mobile device functions can be used to sustain learning. The "*New Media Consortium's higher education edition of the 2012 Horizon Report*" (Cummins *et al.*, 2012) says that mobile applications are the world's fastest-growing feature in the world. This is similar to Norris *et al.* (2011), an exhibition of a collection of important features of the Age of Mobilism, together with being connected almost every time, mobile device affordability and usage across the globe.

There are four factors raised in this study that the IT division can take into consideration when organising learning experiences using mobile devices in the BYOD culture.



### **2.6.1.1 Mobile Device use for Learning Purposes**

As stated by a study carried out by Yarmey (2015), employee respondents at the University of Scranton utilise the mobile opportunity of their smartphones for everyday desktop application functions, including using their mobile phones as a calculating device, in other times as a unit conversion tool, as a dictionary for looking up meaning of words, productivity related micro-apps, such as Microsoft Office, Google Docs. iMessage, amongst others, have also been used by supervisors and co-employees for sharing ideas (Motiwalla, 2007).

### **2.6.1.2 Ease of Communication**

This section focuses on how the mobile device differs from a desktop or even mainframe computers because of its potentials to using the wireless network to access the Internet/Intranet, and how employees can leverage the mobile device to allow them to interact with colleagues within the workplace. This functionality gives employees the potential for instant and sometimes constant feedback by allowing them to interact with colleagues, clients, and access organisation materials from anywhere they have wireless connectivity (Motiwalla, 2007).

### **2.6.1.3 Micro-App Development**

The development of specific micro-apps is made available using software development kits (SDK). In one example reported by Bughin *et al.* (2013), a mobile computing analyst saw the mobile device as a way to streamline lengthy business workflow. A company's dealers and salespeople would meet with various businesses, discuss their needs and then kick off what was usually a 30-day process from application to funding. The process would include providing quotes, approving applications and workflows, and many other steps. This company discovered that by accepting applications, delivering quotes and allowing digital signatures on a mobile device, those 30 days were cut to two. With a sales force of over 10,000 people, that 28-day increase in employee productivity proved to be significant (Bughin *et al.*, 2013).

### **2.6.1.4 Benefits for employees with learning disabilities**

Akour (2009) discussed in his study the benefits that mobile learning at the workplace could have for employees who have learning difficulties. In this section, factors such as the interactive and multi-touch interface of most mobile devices; the wider range and affordable cost of micro-apps; the ability to develop custom microapp to aid self-development are needed to support the idea of being connected anywhere and anytime within an organisation. This set of factors make mobile learning a viable learning medium at self-paced for employees who have learning difficulties.

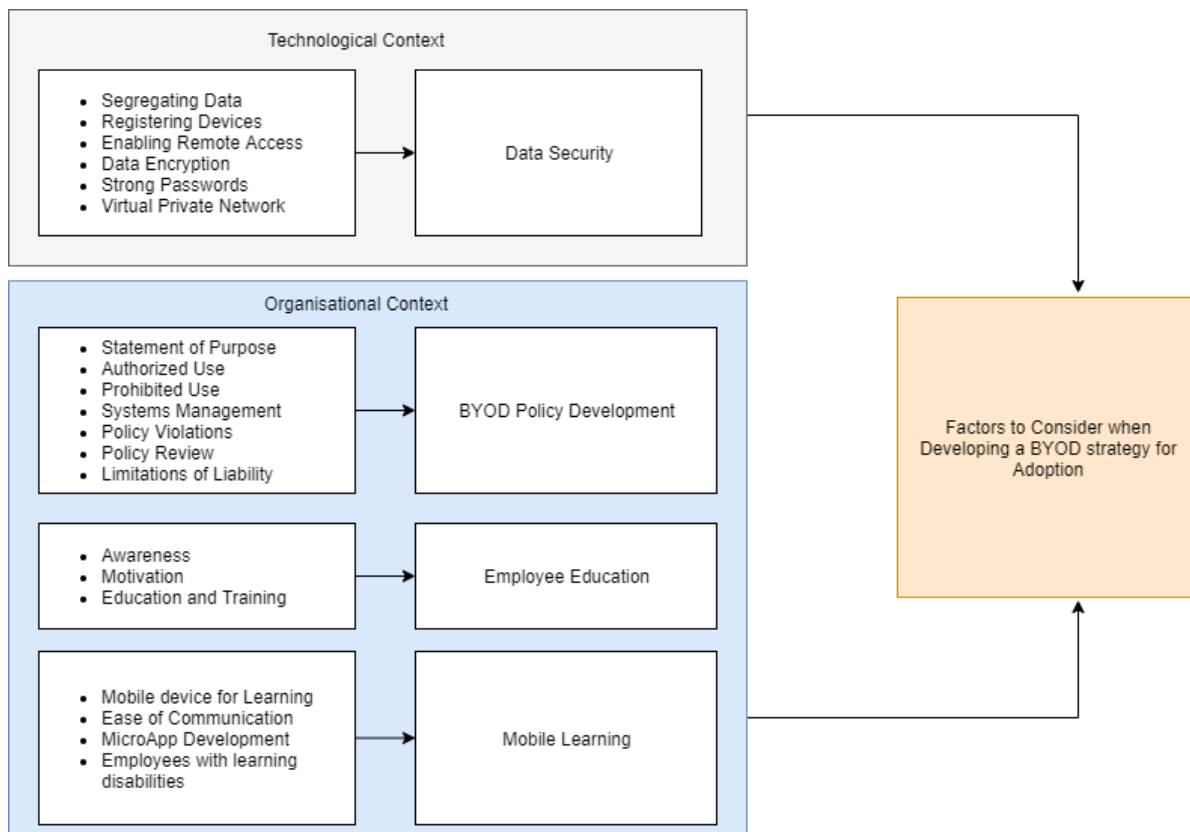
## 2.7 Conceptual Framework for Developing a BYOD Strategy

This study entailed an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets into an organisation. The overall objective of the study is to document a set of factors that need to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of the organisational IT infrastructure. The components identified from the reviewed literature includes data security, employee-education, policy development, and mobile learning.

This study uses the technology-organisation-environment (TOE) (Tornatzky *et al.*, 1990) theory to explore and identify factors to consider when developing a BYOD strategy for adoption in an organisation. TOE describes the process by which a firm implements and adopts technological innovations (Ortbach *et al.*, 2015). The technological context considers both the internal and external existing technologies that might be useful to the company to support an innovation (Oliveira *et al.*, 2011). The organisational context refers to the resources available internally. It considers criteria about an organisation such as scope, size and managerial structure. The environmental context refers to the external factors that impact the organisation strategy such as its industry, interactions with government, and its competitors (Oliveira *et al.*, 2011).

The TOE theory is useful in this study because of its flexibility to explore specific factors when it comes to the development of a BYOD strategy. Of the three contexts, more focus is placed on the organisational and technological contexts as the study's objectives are to identify a set of factors that needs to be considered when an organisation is developing a BYOD strategy for adoption. The environmental context is ignored as the study assumes the external environment/variables is favourable deducing from the literature review on the role of the government in establishing conducive environment for the use of the innovation and also that an organisation has already assessed its social readiness to adopt the innovation.

The literature demonstrated the value of TOE in exploring factors that can be termed as important when developing a BYOD strategy for adoption in an organisation, from this, the researcher proposed a conceptual model for the study as illustrated in figure 2-1 below. The conceptual model is a modified version of the TOE model with the exclusion of the environmental context. Then the research objectives were divided between the two main categories: technology and organisation. As seen below, the primary constructs identified would guide the empirical analysis phase to provide an answer to each research question posed in this study.



**Figure 2-1: Schematic diagram of the Conceptual Framework concerning Factors for developing BYOD Strategy**

The diagram above highlights the components identified from the reviewed literature. These components, best referred to as factors are as explained below:

The component of policy development identifies a collection of features to be used to direct the improvement of policies that addresses the consumption of IT throughout an organisation. Additionally, the subfactors that directly impact on policy development include to how manage: authorised usage of mobile computing devices across the organisation network, prohibit usage of unapproved mobile devices, provision of system management tools/technique of mobile devices, necessary measures for when the policy is violated, guidelines on how often should the policy be reviewed, and how to protect the organisation from any liability that may arise from the use of employees mobile device within the organisation.

Before developing a policy strategy, appropriate data security measures to support an organisation’s BYOD culture needs to be present. The component of data security refers to the safeguarding of private and sensitive data that can be accessed and transmitted by mobile devices within an organisation. Common factors that should be highlighted when it comes to data security includes: an employer’s unauthorised access to both sensitive and private data stored on an employee’s device, an employee’s

unauthorised access to sensitive and private data stored on an employer's network, and the capability of intruders to mimic the user of mobile devices within an organisation trying to gain access to its network.

Exclusive of policy development and data security, employee education for personal mobile device usage within an organisation should try to address employee mindfulness of an organisation's BYOD safety standards and procedures by adopting programs that promotes: employee awareness, employee motivation, and employee education and training on how best to use their personally owned mobile artefacts (smartphones and tablets) within an organisation.

The component of mobile learning viewed the use of mobile devices for knowledge consumption within the organisation. Possible factors involved in this component comprises of employee enthusiasm for learning through mobile devices, the effortlessness of admission and opportunity to learn using a mobile device, the service quality, with regards to dependability and personalisation, and organisation obligation to making learning readily available on mobile.

## **2.8 Validating the Conceptual Framework**

This study aims to identify common factors, as mentioned in the reviewed literature, to explore and identify which of these factors are to be considered important when developing a BYOD strategy for adoption by an organisation.

Before the conceptual framework can be adopted, it is vital to have it validated for its consistency in answering the questions raised by the study. In order to validate that the conceptual framework, which was formed based on theories and existing literature, is consistent with reality, the researcher followed the steps below to ensure that the conceptual framework was validated before data analysis was carried out:

- The researcher seeks comments from supervisor and professors to review the conceptual framework which underpin on previous empirical research that involves the diffusion of BYOD in an organisation.
- The conceptual framework was presented to a panel of researchers in the subject matter, through a Question and Answer session, the conceptual framework was validated with suggestions for improvement.
- The researcher ensured that the factors derived from the conceptual framework are aligned with the research questions and research objectives.
- Evaluation of how the conceptual framework's constructs can be operationalized with an instrument used for data collection was carried out.

- Evaluation of how sampling can be done before an instrument used for data collection was carried out.
- Evaluation of what statistical data analysis needed to be performed once the data is collected was carried out.

## 2.9 Critique

This chapter inspects four designated features of an organisation-wide BYOD strategy for group setting: policy development, data safety, mobile learning, and employee. The objective of this chapter is to offer IT managers an established set of factors that should be taken into account when adopting an organisation-wide BYOD strategy.

However, from the review of existing literature, it was noted that indeed, various studies had been conducted in the areas of BYOD. For instance, from a study launched by Aruba Networks (2012), in Sunnyvale, California, it was conveyed that eighty-four per cent of the hospitals implemented a BYOD strategy to regulate the use of a personal device for work. Although within the hospitals, only seven per cent implemented full access to corporate systems to use applications such as an EMR that is likely to advance rapidly as pressure mounts on IT to open a connection to both physical and other clinical workers. What this study did not indicate is the objectives of the literature and the empirical findings of those objectives.

Ullman (2013) performed a survey entitled "*BYOD strategies: Strategies for K-12 technology leaders*", the survey presented evidence on how to make BYOD programs work. As a result of the description, about thirty-six per cent of the sample size took part in the program; the study reviewed the methods used in implementing a BYOD program by the sampled school districts. Findings showed that users had relative ease with accessing any document they sought to use by using their mobile device. This study, however, did not specify the geographical and sectoral scope for which it was conducted (Ullman, 2013). Also, the survey focused on the strategies employed by technology leaders in improving the concept of BYOD.

Another annotated bibliography carried out by Emery (2012) on "*factors for consideration when developing a BYOD policy in Higher Education*" only proposed a collection of features that IT leaders in higher education management must consider for an institution-wide approach. This current study seeks to employ a qualitative technique in data collection, as data will be collected through the use of an interview instrument. Furthermore, the bibliography by Emery (2012) was carried out in the United States of America with a focus on higher education. The geographical location and target audience of

the study is very much dissimilar in comparison to the scope of the current study; hence, results from the empirical phase would not be similar.

Furthermore, a study carried out by Mwenemeru *et al.* (2014) on developing an ideal guide in the adoption of BYOD in an organisation integrated the Technological, Environment and Organisational (TOE) framework to evaluate the suitability of the notion in the overall functions of the organisation which allowed it to identify whether the notion meets the framework's difficulties so as to enable its successful integration in the day to day activities of an organisation. This study did not test the components from the organisation's landscape in its scope, and it allowed the conceptual framework adopted to act as a guide to presenting a model. The current study, however, identifies common factors, as mentioned in the reviewed literature, to investigate these factors as to its usefulness in the successful integration of personally owned mobile devices within an organisation's infrastructure. These factors will be tested in relation to the adopted conceptual framework, with results educating IT managers on the set of factors needed to implement a BYOD strategy for organisations in South Africa.

## **2.10 Conclusion**

This chapter has introduced the concept of BYOD by explaining what it entails, and it also covers a general review on BYOD. Similarly, it also reviews different literature conducted on the benefits and challenges of adopting a BYOD strategy.

Furthermore, it also reviews the different literature on the adoption of BYOD in the South African IT industry, as well as factors to consider when formulating a BYOD policy framework. Different components of a BYOD strategy were identified and, a fundamental insight into the four pre-selected categories was presented. The current study, however, identifies four common categories mentioned in reviewed literature which requires for the development of a conceptual framework that would guide the study in the investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets into an organisation.

The next chapter presents the research methods, designs and data analysis used to achieve the objectives of this study.

## CHAPTER 3: RESEARCH METHODOLOGY

### 3.1 Introduction

Kothari (2011) defines research methodology as a means to scientifically resolve a research problem. Research methodology encompasses the various techniques, procedures, and steps used by researchers to go about their day-to-day activities of describing, analysing and addressing a research problem (Rajasekar *et al.*, 2006). Therefore, this chapter describes the research design, research method, population, sampling method, sampling technique, sample size, data collection instruments and data analysis procedures used in this study to investigate the factors to consider when developing an organisation-wide BYOD strategy for adoption in organisations in eThekweni Municipal Region, South-Africa.

### 3.2 Research Approach

According to Bhattacharjee (2012), there are two approaches to research; these are the deductive and inductive approach (Saunders *et al.*, 2012). The deductive approach is appropriate when the aim of the research objectives points towards testing an available hypothesis or to validate already known or pre-conceived theories (Saunders *et al.*, 2012). The researcher is tasked with the need to develop a conceptual framework that was used to guide the data collection process towards systematically answering the research questions while also achieving the aims of the research objectives (Bhattacharjee, 2012, Saunders *et al.*, 2012). The inductive approach involves constructing abstract patterns or concepts from empirical observation, while the deductive approach involves the testing of hypothesis or theories (Bhattacharjee, 2012, Saunders *et al.*, 2012).

Adopting the deductive approach, a conceptual framework (see Figure 2.1) was adopted to guide the development of the interview guide used for data collection. The deductive approach allowed the researcher to test the constructs described in the conceptual framework adopted for this study, which led to the identification of themes used in highlighting a set of important factors needed for a BYOD policy development in South Africa.

### 3.3 Research Design

According to Van Wyk (2012), the research design is defined as the overall idea that guides a study. It provides a blueprint for how best to solve the research problem and address the research questions in a

study (De Vaus *et al.*, 2001). According to Bhattacharjee (2012), there are three major types of research designs; they are explanatory research design, exploratory and descriptive research design.

A descriptive research design looks at the what, where, and when about a phenomenon being investigated, which allows for careful observation and documentation of the phenomenon (Bhattacharjee, 2012). It gives the researcher the space to create an accurate profile about events, people and situations.

An explanatory research design is a type of research design that seeks to explain relationships between variables in a study (Gray, 2013). It is best suited for studies that try to understand the association between a dependent variable and an independent variable(s) in a study (Gray, 2013, Saunders *et al.*, 2013).

An exploratory research design is a more in-depth type of research design; it provides a holistic investigation of a problem that is being investigated (Saunders *et al.*, 2013). It allows the researcher the opportunity to critically examine the research problem to provide more insight and to better understand the research problem (Gray, 2013, Van Wyk, 2012). The exploratory research design is most suitable for studies where little or nothing is known about what is being investigated, and it is usually qualitative (Bhattacharjee, 2012, De Vaus *et al.*, 2001).

A descriptive research design, in its form, is known for describing answers to a research problem (Saunders *et al.*, 2013). This type of research design looks at the what, where, and when about a phenomenon being investigated, which allows for careful observation and documentation of the phenomenon (Bhattacharjee, 2012). It gives the researcher the space to create an accurate profile about events, people and situations. This research project adopted a descriptive research design to accurately profile and document the set of factors to be considered when developing the BYOD strategy for use in an organisation in South Africa.

### **3.4 Research Method**

Research method refers to an approach or procedure followed in a study (Saunders *et al.*, 2013). There are two types of research method; they are quantitative and qualitative research method.

The quantitative research method is a research method that involves testing theories or investigating the relationship between variables in a study (Saunders *et al.*, 2013). It uses large samples and results can be generalised based on the large samples. Quantitative research mostly deals with quantity and



measurement, and it is expressed numerically (Lakshman *et al.*, 2000). Data collection is done using a questionnaire, and it is usually in the form of numbers, and the results are analysed using statistical analysis (Saunders *et al.*, 2012).

As compared to a quantitative method, a qualitative research method offers a more holistic approach (Lakshman *et al.*, 2000). It provides a better understanding, a more fruitful and profound insight into the research problem because it allows the researcher to interact directly with the target population (De Vaus *et al.*, 2001); hence, the researcher has first-hand knowledge of the problem that is being investigated (Saunders *et al.*, 2012). It uses fewer respondents compared to a quantitative method, and data is collected through observations, focus group discussion and interviews (Lakshman *et al.*, 2000). Data collected in the qualitative method is analysed using a thematic analysis.

The qualitative research method because of its potential in identifying grounded concepts was considered as the most suitable research method for this study as it aims to get a rich, robust and detailed information about the set of factors to consider when developing an organisation-wide BYOD strategy for organisations in South-Africa. Moreover, since senior managers with titles such as Chief Technology Officer (CTO), Chief Executive Officer (CEO), and Chief Information Officer (CIO) can decide to allow employees to bring their own personally owned mobile artefacts such as tablets, smartphones and use them within the organisation, opinions from senior management were elicited for this study.

### **3.5 Research Site and Setting**

According to Sekaran *et al.* (2013), a research site is defined as the location where a study is conducted. The research site for this study is the eThekweni Municipal Region (the region with the highest urban population and the economic hub of the province) of the KwaZulu-Natal province, South Africa. The research setting is defined as the place where the data for a study is collected (Sekaran *et al.*, 2013). The research setting for this study are organisations from the research site that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. These organisations drive financial revenue through the values generated by the adoption of IT as a business enabler. Hence, they can provide the required information on the factors to consider when developing an organisation-wide BYOD strategy for adoption in organisations in eThekweni Municipal Region, South-Africa.

### 3.6 Population of the study

The population of a study refers to a group of people that a researcher is interested in studying (Sekaran *et al.*, 2013). It is a group of individuals where data/information for a study is obtained (Bhattacharjee, 2012). The population for this study were various organisations from the research site that either considers IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does.

According to Rajasekar *et al.* (2006), the target population is the specific people that a researcher is interested in studying. Hulley *et al.* (2013) also defined the target population as specific people with common characteristics where data for a study is obtained. The target population for this study was CIO's and CTO's working in organisations that are involved in core IT strategy in eThekweni Municipal Region, South-Africa.

In this study, the CIO's and CTO's were chosen as the target population because these people, based on their position, years of experience and expertise are knowledgeable about what factors are needed when formulating a BYOD strategy for adoption in organisations in eThekweni Municipal Region, South-Africa. Therefore, they can provide robust information about the required information needed by the researcher.

### 3.7 Sampling and sampling technique

Sampling is the procedure for selecting samples from a population (Gill *et al.*, 2010). Lunsford *et al.* (1995) described sampling as methods and criteria a researcher can use to select participants for their research. The samples selected are a representation of the whole population. There are two categories of sampling technique: probability and non- probability sampling.

In probability sampling, all the elements in the target population have an equal chance of being selected to participate in a study (Lunsford *et al.*, 1995). While in a non-probability sampling technique, all the elements in the target population do not have an equal chance of being selected to participate in a study (Lunsford *et al.*, 1995).

Non-Probability sampling was adopted in this study because all the staff in the organisation do not have an equal chance of being selected to provide the required information about the factors to consider when developing an organisation-wide BYOD strategy for adoption in the organisation. In other words, the

required information was gotten from individual staff with some specific characteristics and experience using a purposive sampling technique.

Purposive sampling technique also called judgmental technique is a type of non-probability sampling where a researcher selects samples based on specific characteristics or traits exhibited by individuals or group of individuals (Guarte *et al.*, 2006). Purposive sampling technique gives room for the researcher to select individuals or group of individuals who will provide detailed, robust and rich information about the research questions asked in the study (Devers *et al.*, 2000). A purposive sampling technique was selected in selecting CIO's and CTO's in organisations because they can provide the required information needed to address the research questions in this study. This ultimately gave room for more accurate and realistic information about the factors to consider when developing an organisation-wide BYOD strategy for adoption in organisations in eThekweni Municipal Region, South-Africa.

### **3.8 Sample and Sample Size**

Sample denotes a part of the population chosen to join in a study (Lunsford *et al.*, 1995). The samples for this study were drawn from various organisations involved in core IT strategy in eThekweni Municipal Region, South Africa.

The sample size is the total sum of subjects nominated to participate in a study (Sekaran *et al.*, 2013). According to Patton (1990), there are no specified rules for measuring the sample size in qualitative research; it is dependent on the dimensions (breadth or depth) in which the researcher seeks to inquire. Out of the 24 organisations selected to participate in the study, only 14 organisations agreed to participate, which conforms with Guest *et al.* (2006) experiment with data saturation and variability, who indicated that 14 participants satisfy the sample size requirement for a qualitative study using in-depth interviews for data collection from a homogenous population. Hence, the sample size for this study was fourteen (14) individuals who were drawn across fourteen (14) different organisations in eThekweni Municipal Region, South-Africa that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does.

These organisations drive the company's revenue through the values generated by the adoption of IT as a business enabler. Hence, they can provide the required information on the factors to consider when developing an organisation-wide BYOD strategy for adoption.

### 3.9 Participants' Demographics

In order to achieve the objective of this study, selected participants from fourteen (14) small to medium sized organisations in eThekweni Municipal Region, South Africa were interviewed. Table 3.1 presents the profile of the participants of the study.

**Table 3.1: Profile of participants**

Organisational level	Organisational Sectors	Quantity	Experience	Qualifications
Executive	eCommerce, General Clothing, Transportation, Business Process Outsourcing, Manufacturing	4	15 – 20 years	All the participants of this study had undergone training and attained certifications in one or more IT management fields including IT governance, IT security, IT Audit. Participants are also certified in at least one of the following certifications; Control objectives for information related technology (COBIT), Information technology infrastructure library (ITIL), Certified information security manager (CISM), Certified in the governance of enterprise IT (CGEIT) and Certified information systems auditor (CISA).
Management	eCommerce, General Clothing, Transportation, Business Process Outsourcing, Manufacturing	8	10 – 16 years	
Operations	eCommerce, General Clothing, Transportation, Business Process Outsourcing, Manufacturing	2	4 – 10 years	

### 3.10 Data Collection

This study adopted a descriptive research design and a qualitative research method; hence, data was collected through the process of conducting interviews. Interviews were conducted among 14 respondents who were drawn using purposive sampling technique from 14 different organisations in eThekweni Municipal Region, South-Africa that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. The use of interview as a means for data collection enabled the researcher to gather rich, in-depth and robust information to document the factors to consider when developing an organisation-wide BYOD strategy for adoption in organisations in eThekweni Municipal Region, South Africa.

### **3.10.1 Interview**

Wallen *et al.* (2013) describe "*interview*" as a form of research in which individuals are questioned orally. It is a form of two-way communication concerning the researcher (interviewer) and the respondents (interviewee). The process of conducting interviews enable respondents to share their opinions or views about a phenomenon or research problem identified by the researcher (Wahyuni, 2012).

This study adopted a standardised open-ended interview to investigate the factors to consider when developing an organisation-wide BYOD strategy for adoption in the organisation in eThekweni Municipal Region, South-Africa. An open-ended interview allows the researcher to draft a set of open-ended questions that participants can respond to sequentially. This interview method was adopted since it helps target the specific phenomenon the researcher is investigating. The objective was to gather as much correct information regarding the phenomenon being investigated without having to do a follow-up interview for missed or forgotten questions. Furthermore, the reliability of the answers provided can best be achieved by adopting a standardised open-ended interview approach since the questions were asked in a set order. This reliability increases the trustworthiness of the answers provided to answer the research questions raised in this study accurately. While the standardised open-ended interview approach brings about structure to the interview process, the descriptive objective of the study was preserved by making the question, and answer process flexible such that participants were allowed to skip some of the questions they feel have already been addressed from previous responses.

### **3.10.2 Interview Schedule**

The interview schedule is a document used by a researcher to guide an interview process (Morehouse *et al.*, 2002). It could comprise of different types of questions including fixed alternatives, open-ended and scale items (Kerlinger, 1970), which could be grouped into sections of different criteria such as experience, demographics, knowledge and descriptions (Patton, 1990). The questions in the interview schedule of this study were crafted in line with the research framework that was adopted to guide the data collection process. A pilot study was conducted with two IT practitioners that did not form part of the sampled respondents to assess the coherence of the questions to the research framework and the clarity of the questions. The interview questions were repeatedly revised by both the researcher and the supervisor, according to the feedback received from the pilot study and received approval from the University of KwaZulu-Natal (UKZN) Ethics Committee.

After the supervisor approved the interview questions, the revised interview questions document was emailed to all the target population identified in the study. This was done in order for the respondents

to familiarise themselves with the interview questions. One week later, a follow-up email was sent to inquire if the respondents needed clarifications on some of the interview questions, and all the respondents required no clarifications. Two weeks later, a follow-up email was sent to all the respondents in order to schedule the interview date. The interview process was conducted in a quiet and serene environment, and it lasted for about thirty (30) minutes and was completed in six (6) weeks. An audio recorder, a pen, and jotter were used to take notes during the interviewing process. The interview questions document can be viewed in the appendix (Appendix C).

The interview questions encompass the primary objective of the study which is to review the factors to be considered before implementing a BYOD policy for portable devices used by an organisation's staff in relation to the four significant categories chosen concerning the consumerization of IT (a) policy framework. (b) data security, (c) employee training, and (d) mobile learning at work

### **3.11 Ensuring Reliability and Validity**

Research reliability refers to the degree in which the outcomes of a study are consistent when repeated (Golafshani, 2003b), while validity refers to how accurate the results of a study are (Joppe, 2000). Reliability and validity tests are most commonly used in a quantitative research study because they are used to test the accuracy of the research instruments – a questionnaire, unlike a qualitative study which uses an interview to gather data.

Golafshani (2003b) argued that reliability and validity tests do not apply correctly in a qualitative research study because the researcher is part of the process. Therefore, triangulation, credibility, transferability, dependability, and confirmability are essential criteria to test for reliability and validity in a qualitative research study, as suggested by (Wahyuni, 2012). These processes are discussed below:

#### **3.11.1 Triangulation**

Research triangulation attempts to ensure the validity and reliability of a qualitative study, and it requires the researcher to cross-reference or cross verify the same information by employing multiple data sources (Shenton, 2004). In line with this, triangulation was achieved by employing participants from 14 various organisations, to minimise the consequence on the study of certain local factors specific to one organisation. The results obtained from the participants from the various organisations were cross-referenced against each other to ensure that the findings obtained have greater credibility in the eyes of any reader.

### **3.11.2 Credibility (Internal Validity)**

Credibility, also called accuracy ascertains whether a study or test measures what is intended to measure (Wahyuni, 2012). It ascertains whether the result of a study is an accurate reflection of the population. Wahyuni (2012) suggests that, for a study to be considered credible, the population where data is collected plays a significant role because they are involved with what the researchers intend to investigate, therefore they can provide the accurate and necessary information.

Credibility was ensured in this study by targeting organisations in eThekweni Municipal Region, South-Africa that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. These organisations were chosen because they drive the company's revenue through the use of IT tools; hence, they can provide the necessary information about the factors to consider when developing an organisation-wide BYOD strategy for adoption.

### **3.11.3 Transferability (External Validity)**

Transferability, also called generalisability in a qualitative study denotes the extent that the conclusions from a study can be generalised to other comparable studies (De Vaus *et al.*, 2001). Golafshani (2003a) opine that generalizability in a qualitative study depends on the samples selected to participate in the study. Wahyuni (2012) also emphasise that if the subjects that participated in a study have certain traits or characteristics needed to provide information; hence, the results can be generalised to other similar studies. Hence, if related research works on the factors for consideration when developing a BYOD policy for adoption in organisations in eThekweni Municipal Region, South Africa show similar results, the likelihood of applying this study to general happenings or situations can be put forward. The broad mix of the participants from various organisations during the in-depth interviews also give some pointers to the transferability of this study. During the use of qualitative research instruments (i.e. in-depth interviews), the purpose of the sampling process is to capture several happenings and engage CIO's and CTO's who were chosen as the target population because these people, based on their position, years of experience and expertise are knowledgeable about the factors to consider when formulating a BYOD strategy for adoption in organisations in eThekweni Municipal Region, South-Africa.

### **3.11.4 Dependability (Reliability)**

Dependability is the extent to which the study is consistent and repeatable. One of the significant ways of improving the dependability of a study is through an external audit (Lincoln, 1985). An external audit

has an independent researcher review the methods and activities used in achieving the overall objectives of the research.

This study ensured dependability before sending off to an independent researcher. The steps taken to achieve dependability are detailed below:

- A pilot study was conducted with two IT practitioners that did not form part of the sampled respondents to assess the coherence of the questions to the research framework and the clarity of the questions.
- After receiving feedback from the pilot study process, both the researcher and the supervisor repeatedly revised the interview in order to address the problem that is being investigated suitably.
- After the supervisor approved the interview questions, the revised interview questions document was emailed to all the target population identified in the study. This was done in order for the respondents to familiarise themselves with the interview questions.
- One week later, a follow-up email was sent to inquire if the respondents needed clarifications on the interview questions, and all the respondents required no clarifications.
- Two weeks later, a follow-up email was forwarded to all the respondents in order to schedule the interview date.
- The interview process was conducted in a quiet and serene environment, and it lasted for about thirty (30) minutes and was completed in six (6) weeks.
- An audio recorder, a pen, and jotter were used to take notes during the interviewing sessions.
- At the end of the interviewing session, the researcher played back the documented audio to ascertain the content.
- The researcher (interviewer) also compared the notes taken during the interviewing process with the recorded audio.
- The research collection instruments, findings and analysis were sent to an independent researcher (selected based on experience and expertise in qualitative research) to evaluate the accuracy and coherence of the interviews, findings and conclusion.

### **3.11.5 Confirmability (Objectivity)**

Confirmability ensures that the results of a study are an accurate reflection of the participants' and not the researchers' (Wahyuni, 2012). Confirmability gives room for others to confirm the authenticity of the findings of a study. Documentation, a record of research progress should be kept, which serves as an audit trail for examination (Wahyuni, 2012).



All data/information gotten from respondents during the process of conducting this study are available on an audio recorder and will be handed to the School of Management, IT and Governance which will be then be archived for five years.

### 3.12 Data Analysis

Data analysis is the process of extracting meaningful information from a data corpus. The data collected for this study were analysed using the thematic analysis. The thematic analysis is a qualitative analytic/analysis method used by researchers to gain insight and generate knowledge from a qualitative data set (Braun *et al.*, 2006). Using the thematic analysis for this study, the collected data from the interviews were analysed and reported in sections of identified patterns known as themes.

The thematic analysis could be inductive or deductive in approach. According to Fereday *et al.* (2006), the deductive approach is the use of a theoretical/conceptual framework to inform and guide the generation of codes and themes from a dataset, while the inductive approach, on the other hand, is content driven, such that the codes and themes are generated from the dataset and not underpinned by a theoretical/conceptual framework. The deductive analysis is suitable for this study as it allows the researcher to describe results from the interview transcript while being guided by a conceptual framework.

#### 3.12.1 Thematic Analysis Phases

The six steps of conducting qualitative data analysis as identified by Strauss *et al.* (1998) and Braun *et al.* (2006) was adopted for this study. The steps adopted are as follows:

- a. **Familiarisation with the data:** This process involves the researcher associating himself/herself with the collected data. According to Lacey *et al.* (2001), a researcher is expected to get familiar with data gathered from respondents to allow for an in-depth understanding of the collected data. A researcher can achieve familiarity through the process of transcribing the interviews themselves and re-reading the data set over again (Lacey *et al.*, 2001). In the event where the researcher has outsourced the transcription of the interview data collected, he/she is tasked with the responsibility of crosschecking the accuracy of the transcript by listening to the interview when reading the transcribed data. To achieve complete familiarity with the data corpus, the researcher is advised to not only transcribe the interview data but to read the interview transcript repeatedly before continuing onto the next phase.
- b. **Coding:** In this stage, it is believed the researcher has familiarised himself/herself with the data set and has generated a list of ideas about the content of the data, most notably the relevant aspects of them. This stage concerns itself with the generation and extraction of ideas, patterns

and relationship from the data set (Saldaña, 2015). The generation of initial ideas, patterns and relationship should be guided by the research objectives and labelled correctly for better understanding. This process could be done manually or facilitated by a qualitative data analytics software such as NVivo or Atlas (Saldaña, 2015) For this study, NVivo was used to facilitate the generation of labels that identify important features of the data relevance to participants response to the research question. After coding the interview transcripts, relevant codes and excerpts were collated

- c. **Searching for Themes:** This stage begins immediately after all data has been collated and coded into a list of various codes that have been identified from the data set. This stage ensures a process of reviewing the generated labels for a broader meaning is followed. This process also involves discarding irrelevant labels, while redundant labels are merged and given higher-level descriptions as temporary themes. In this study, original labels were examined for redundancy, irrelevancy and relationships. The revised labels were marked as candidate themes.
- d. **Reviewing Themes:** At this stage, the examination of the candidate themes was further refined to determine if they need further revision by rewording, splitting, or discarding. For this study's purpose, candidate themes were examined for appropriateness. Mind maps and hierarchical chart were used to conceptualise the pattern and relationship between the candidate themes.
- e. **Defining and Naming Themes:** This stage begins as soon as the investigator has an adequate thematic map of the data. The researcher performs a final check on the appropriateness of the themes and their relationships. At this stage of the study, candidate themes were re-examined for appropriateness, and final themes of the study were drawn up based on the frequency of response from respondents. A detailed analysis of the themes was composed concerning how they answer the research questions.
- f. **Writing the report:** It can be agreed to that at this stage, the investigator already has a set of themes before proceeding to commence work on the final analysis and write up for the dissertation (Clarke *et al.*, 2013). In this dissertation, the researcher composed a discursive narrative of themes in relation to the study's objectives, existing literature, and the conceptual framework adopted by the researcher. The analysis of the themes was discussed using existing literature on BYOD policies.

### 3.12.2 Themes of Analysis

The themes selected for this study were driven by the conceptual framework adopted by the researcher, and the responses from the various personnel interviewed. The four broad themes that were identified are as follows:

1. Factors to be considered when adopting a policy for the acceptable and prohibited usage of a personally owned mobile handheld device within an organisation.

2. Factors allowed to determine relevant factors to be taken to guarantee an organisation's data is secure while consenting to the utilisation of individually owned portable electronic devices in the workplace.
3. The right methods for consideration in raising employee awareness of safety standards and regulations when using a personally owned mobile device.
4. The right modality that can be incorporated when crafting drafting work learning experiences that appeals to the unique technical elements of mobile artefacts in the workplace.

### 3.13 Ethical Consideration

Brenda *et al.* (2003) describe ethics as the code or guidelines that aid a researcher in conducting responsible research. It allows the monitoring and educating of researchers in other to ensure that a high ethical standard during research is maintained. It ensures that researchers have the safety and dignity of their respondents in mind and not solely for obtaining vital information.

For this study, the researcher obtained a gate keeper's letter to conduct the interview with all the organisations identified in the target population. After the gate keeper's letter was issued, a copy of the letter was attached with the interview questions and sent to the ethics board of the University for the permission to conduct the study. An ethical authorisation was issued by the ethical committee of the University, granting the researcher consent to conduct the interview. The ethical letter document can be seen in the appendix (Appendix A).

To ensure that the safety and dignity of respondents are maintained, an informed content was required from the respondents either by giving oral or written consent to show their willingness to take part in the study after the researcher has elaborately given them a great idea of what they would be involved in.

The ethics of privacy and confidentiality of the respondents was maintained by reminding them of the power they have in deciding whether their information should be provided to the public or not, and also the capability to limit access to personal information.

Similarly, in order to ensure the safety of the respondents, the ethics of anonymity was maintained. Anonymity, in this case, would involve not releasing the names of the respondents when presenting the findings or results without their permission. It would also involve the protection of any information that would identify the respondents, which might include office address, occupation.

### 3.14 **Conclusion**

This chapter talks about the research methodology adopted in this study. The different types of research methods, approach, designs, and procedures were explained, and the reason for using a particular approach, design, and procedure selection were justified. This chapter also described the sample, sample size, and sampling technique adopted in this study. Similarly, the interview process, schedule, and the various techniques used to test for reliability and validity were explained. The ethical consideration was also described. The next chapter presents an in-depth analysis of the findings and results obtained following the data collection process.

## CHAPTER 4: DATA PRESENTATION AND ANALYSIS

### 4.1 Introduction

This study entails an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets into an organisation. The overall objective of the study is to document a set of factors that need to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of the organisational IT infrastructure. This study is qualitative; hence, interviews were used to elicit information from respondents. This chapter outlays and analyses the data collected in this study to address the research questions identified below holistically:

- What factors are to be taken into account when adopting a **policy** for the satisfactory usage and prohibited use of personally owned portable handheld devices?
- What factors should be reviewed to ensure an organisation's data is **secure** while allowing the operation of personal devices by employees?
- What approach must be taken into account in order to raise **employee awareness** of safety benchmarks and pronouncements in the use of portable personal devices?
- What modality should be factored in when designing a **work learning experience** that satisfies the unique technical elements of portable devices?

### 4.2 Conceptual Framework

After carefully reviewing the literature, this study identified four pre-selected factors that are needed to be considered for a BYOD strategy to be effectively adopted by an organisation. The proposed factors include data security, policy development, employee education, and mobile learning. As conceptualised in figure 4.1 below, an organisation's BYOD strategy is said to consist of four main components. The components are categorised into two main themes: technology and organisation. The components of these themes, best referred to as constructs, are explained below:

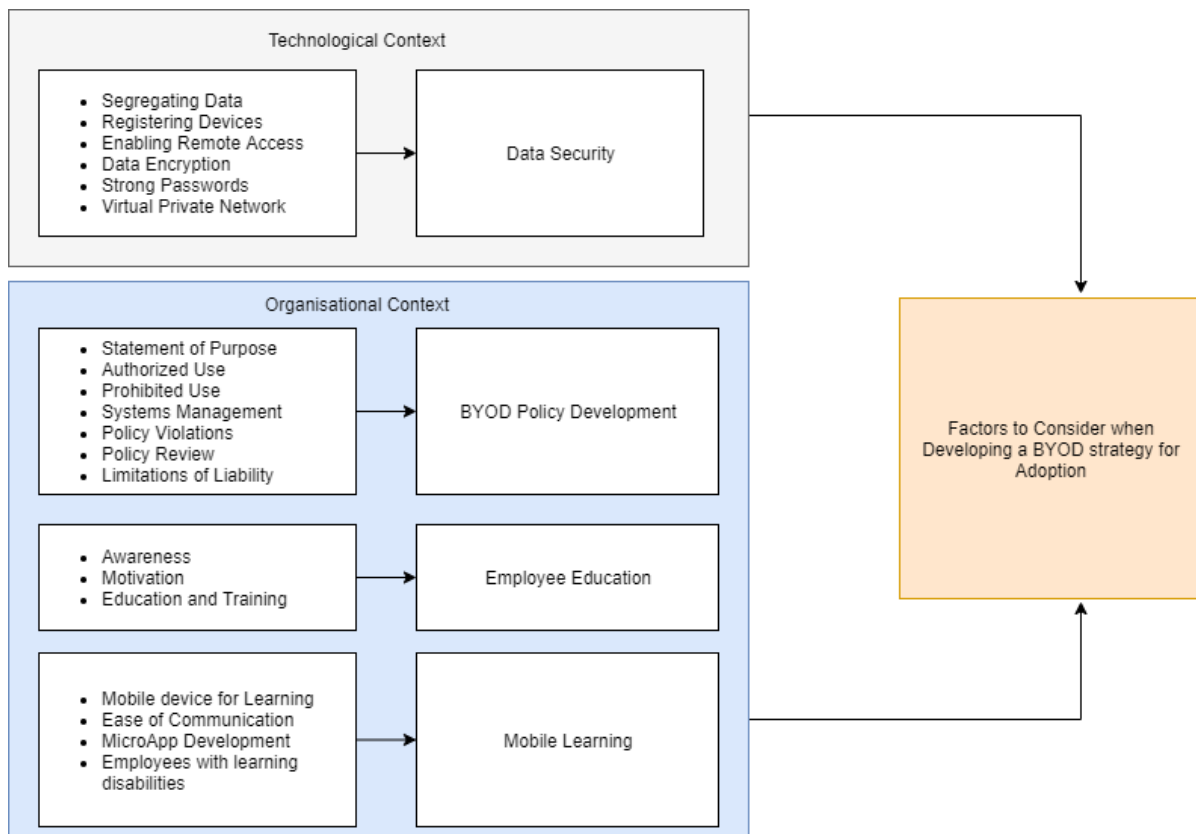
**1<sup>st</sup> Construct – Data Security** – Before developing a policy strategy, appropriate data security measures to support an organisation's BYOD culture needs to be present. The component of data security refers to the safeguarding of private and sensitive data that can be accessed and transmitted by mobile devices within an organisation. Common factors that should be highlighted when it comes to data security includes: an employer's unauthorised access to both sensitive and private data stored on an employee's device, an employee's unauthorised access to sensitive and private data stored on an

employer's network, and the capability of intruders to mimic the user of mobile devices within an organisation trying to gain access to its network.

**2<sup>nd</sup> Construct – Policy Development** – The component of policy development identifies a collection of features to be used to direct the improvement of policies that addresses the consumption of IT throughout an organisation. At the same time, the factors that directly impact on policy development include to how manage: authorised usage of mobile computing devices across the organisation network, prohibit usage of unapproved mobile devices, provision of system management tools/technique of mobile devices, necessary measures for when the policy is violated, guidelines on how often should the policy be reviewed, and how to protect the organisation from any liability that may arise from the use of employees mobile device within the organisation.

**3<sup>rd</sup> Construct – Employee Education** – Exclusive of policy development and data security, employee education for personal mobile device usage within an organisation should try to address employee mindfulness of an organisation's BYOD safety standards and procedures by adopting programs that promotes: employee awareness, employee motivation, and employee education and training on how best to use their mobile devices within an organisation's network.

**4<sup>th</sup> Construct – Mobile Learning** – The component of mobile learning looks at the usage of mobile devices for knowledge sharing and consumption within an organisation. Possible factors involved in this section comprises of using the mobile device for learning purposes within an organisation, how mobile device helps employees with learning disabilities, how the mobile device can be used to aid micro-app development and most importantly on how it helps support existing communication channels within the organisation with the sole aim of making it easy to facilitate communication.



**Figure 4-1: Schematic diagram of the adopted Conceptual Framework concerning Factors for developing BYOD Strategy.**

Each of the section below encompasses the constructs in the conceptual framework, and this ultimately addressed each research questions. Thematic analysis was utilised to analyse the responses of the various participants. The themes that were dominant from the analysis are discussed in the context of the reviewed literature and are presented under each construct described in the conceptual framework adopted by this study.

### 4.3 Policy

There are several factors to consider when applying the principle of using mobile devices that are acceptable and prohibited. IT managers need to contemplate these factors when designing a strategy for using personally owned mobile artefacts such as smartphones and tablets in the organisation.

A quality BYOD policy offers comprehensive, targeted management to educate all members of the organisation in the use of personally owned mobile artefacts (smartphones and tablets) within the organisation. The policy should introduce the organisation's central resource-use philosophy. It ought to guarantee members of the organisation that its resolution is not to create a base for administrative implementation or legal action but to deliver a mutual understanding of the objectives for which an

employee can and cannot use the resources.

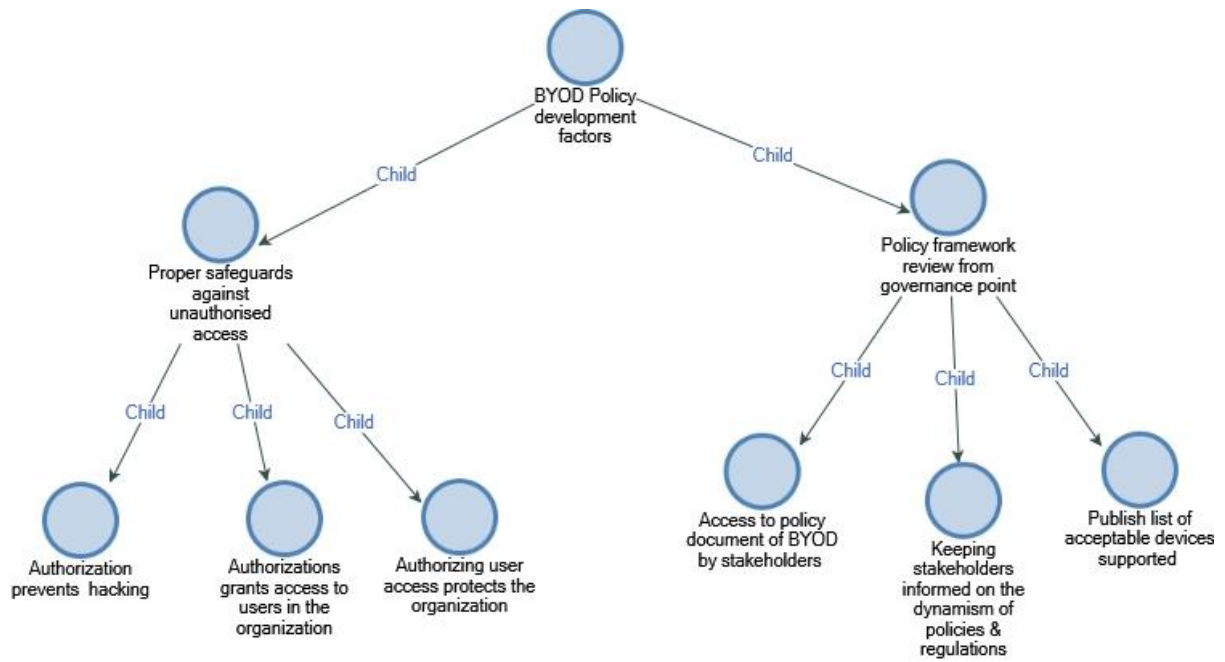
From the responses, the most common themes, identified from the frequency of positive responses from all 14 participants, that should be considered when adopting a policy for the acceptable and prohibited usage of a mobile device in an organisation can be categorised into authorised usage, systems management, policy review and limitation of liability. This is shown in Table 4.1 below:

**Table 4-1: Factors to consider when adopting a policy for acceptable and restricted mobile usage in an organisation.**

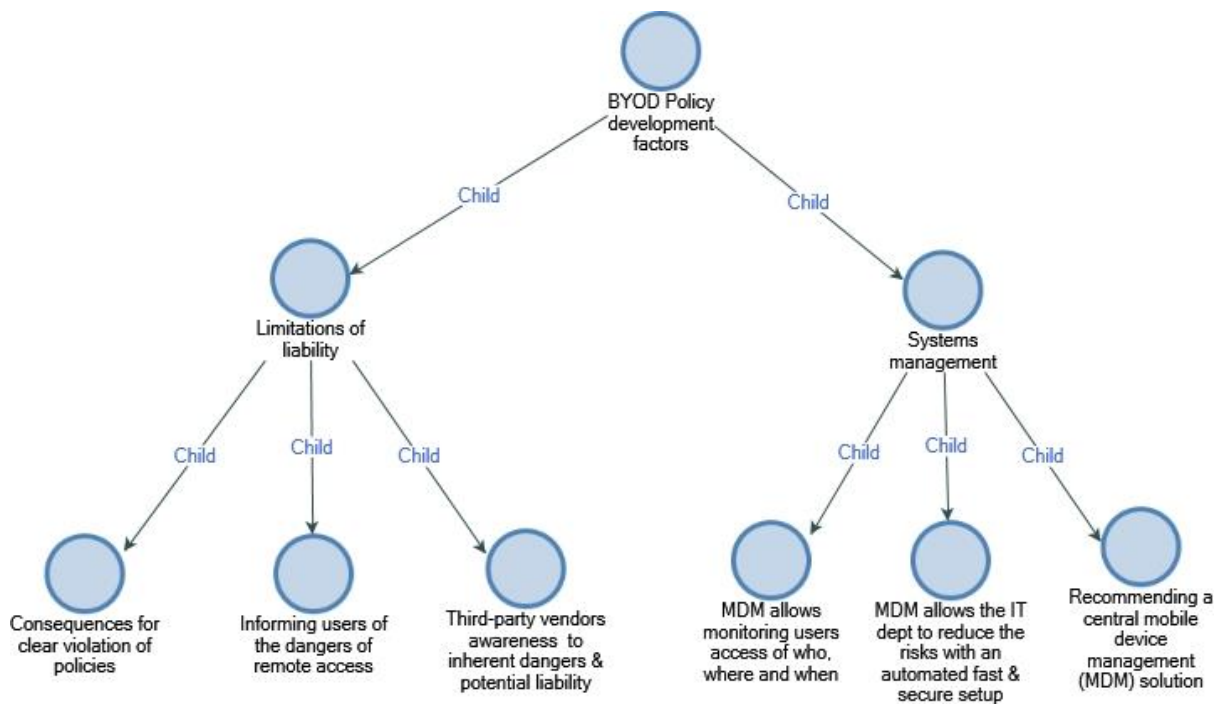
<b>Themes</b>	<b>Frequency of Positive Responses</b>
Authorised Usage	6
Systems Management	9
Policy review	4
Limitations of Liability	3
Statement of Purpose	2
Policy Violations	1
Prohibited Use	2

As further illustrated in Figure 4-2 and Figure 4-3 below, four sub-themes were identified as important themes based on the frequency of their responses. These sub-themes and their relationship to this study's objectives are presented below.





**Figure 4-2 Policy development factors and BYOD I**



**Figure 4-3 Policy development factors and BYOD II**

### 4.3.1 Authorised Usage

This section talks on what type of technology and tools can be used within the organisation and who the authorised users are. As reported by Emery (2012), an organisation must have a defined list of authorised users (employees, vendors, and partners), mobile devices, and technology to allow in the

workplace. Furthermore, this part should define the fair and responsible use of mobile devices within the organisation (Emery, 2012). If the IT division deems it fit to make provision for some resourceful use of its network for activities such as access to employees' e-mail(s) account, such use must be precisely permissible for, and defined, in the policy document.

Respondents explained that a significant number of stolen and misplaced devices means that the attacker can access the actual hardware of the device. This is a different type of as compared to stationary devices, such as servers and workstations, which are less likely to be accessed remotely. For instance, respondent eight (8) stated that:

*“Unprotected devices can pose some severe security risks and can serve as an entry point for hackers seeking access to otherwise secure networks. Properly securing our network did include: having a clear email security policy. For example, not letting users download large archived files from a mobile device, as this may be a sign of unauthorised access.”*

Forty-two per cent of the respondents stated that it is difficult to protect the device after the intruder has gained admission. Therefore, physical hardware, operating systems, and applications affect the generic security components of the mobile artefacts and this hazard upsurges when employees bring potentially unsafe and old mobile devices into the organisation. One of the respondents believed that many of the staff members are welcoming the BYOD idea, thus, in order for an organisation to remain flexible and adaptable when it comes to receiving these employee-owned devices into its network surroundings, it is important to explain to the workforce; who the authorised users are, and what type of technology can be used on their respective devices. According to respondent two (2) who stated:

*General IT supportability of BYOD environments is difficult as a result of the large variety of personal devices, platforms, and operating systems. Today, so much messaging is happening over collaboration applications, such as Skype or iMessage, and some of these applications use transport encryption that is not easily intercepted, and most organisations are not set up to regulate their usage. Our IT department mitigates these risks and challenges by managing device and application settings to ensure data integrity and security and also offering secure and reliable internet experience.”*

In a BYOD scenario, this hazard has been highlighted, as organisations failing to set the minimum requirements for personal devices may have more insecure mobile devices available to access organisational data. Not many devices have reliable architecture set-up as compared to features found in laptops and other desktop devices, and also there is the issue of jailbreaking by bypassing security and operating system-based limitations on the mobile devices. Respondent ten (10) opined that:

*“We do have relevant acceptable use policies that also describe devices that are prohibited from accessing our network, especially devices that are jailbroken.”*

Another method is to create a list of supported mobile artefacts and mobile application platforms before allowing it to be used in the workplace. All user devices are expected to be registered for use within the organisation before allowing access to the network. Although it is ideal for organisations looking to implement a BYOD strategy to try and create an environment where any mobile devices are supported, it is still useful to have a list of supported devices and platforms. This responsibility lies on the IT division, to determine a published list of supported mobile artefacts and mobile application platforms and to permit employees to use their device as long as it matches pre-approved devices on the list. As reported by respondent five (5) who said:

*“We have a BYOD policy in place that includes mobile device management, which gives IT access to any devices that may access our business network along with the capability to revoke access or even wipe a device if it is lost or stolen, and outlines policies and protocols for accessing company data from remote locations.”*

Additionally, some respondents believed that even though social applications (Facebook Messenger, Twitter direct messaging and LinkedIn Mail) are frequently allowed for business communications, organisations are still left with the task of adequately securing their own information system through proper labelling and identification of any possible restrictions to the BYOD strategy, such as operating systems, approved devices, cloud services and operating system versions. As shared by respondent eleven (11) who stated that:

*“We specify the types of personal data that can be accessed, as well as which devices can be used. The more specific we are, the better – we want to avoid any miscommunication regarding proper usage so that our confidential company data is as secure as possible. It is recommended that antivirus software is installed on personal devices, and technical support is provided to employees on their devices.”*

It is unfeasible for an organisation's IT support centre to assist devices running a large variety of operating systems with a wide variety of configuration settings from an enormous diversity of manufacturers. Therefore, the sum of special provision provided to employees' hinges on the organisation's personnel means, whether devices are registered on a corporately-approved shortlist of devices, and the degree to which devices are essential for employees to accomplish their job. One of the respondents stated that:

*“The mobile device market is very unpredictable, we cannot but cater for all types of device in the policy, there would be no need in the first place, as research on what these devices do can consume resources we do not have. We do not know the types of devices these employees are going to be bringing in, and we will not be forced to be preferential to some and neglect others because we could not allow the usage of those devices. However, what we have done is to*

*correctly determine and communicate the intended and acceptable use of privately-owned devices, as well as specify which devices and operating systems are supported, and when new ones will be added.”*

### **4.3.2 Systems Management**

This segment touches on the employees' relationship with an organisation's systems management. According to Emery (2012), an organisation should have detailed instructions to document the use of e-mail and electronic documents and storage of those documents. One example would see a section that talks on enforcing power-on authentication for a user's mobile artefact before use on an organisation's network. This section should notify all user groups (employee, and systems administrators) of their accountability so that they know what they are liable for.

Organisations who are going to be using a Mobile Device Management (MDM) solution need to have a centralised administration panel that should at least provide support for the leading mobile operating systems, like the Windows Mobile, Android, and Apple iOS. Respondent one (1) had the following to say:

*“It is important for organisations to adopt a central device management tool that controls, monitors at the very least the usage of devices across our networks and data house. MDM is a way to ensure employees stay productive and do not breach corporate policies. Many organisations control the activities of their employees using MDM products/services. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on devices, enforcing corporate policies, integrating and managing mobile devices including laptops and handhelds of various categories. We are looking at adopting a cloud-based solution.”*

Similarly, respondent seven (7) also reported the following:

*“Mobile device management is an important factor. It is like adding an extra layer of security and ensuring a way to monitor device related activities. MDM provides device platform-specific features like device encryption, platform-specific policies, SD Card encryption. Geo-location tracking, connectivity profiles (VPN, Wi-Fi, Bluetooth) and plenty other features are part of MDM Suite. Present day MDM solutions offer both software as a service (SaaS) and on-premises models. Our SaaS (cloud-based) systems were quicker to set up, offer easier updates with lower capital costs compared to on-premises solutions which require hardware or virtual machines, need regular software maintenance, and might incur higher capital costs.”*

MDM vendors now offer cloud versions of their software for use. These cloud versions, however, may

be restricted in the number of devices they can allow, thereby allowing small organisations to have access to the important functionalities at a reasonable price. Apart from having to decide between standard and cloud MDM solutions, an organisation needs also to determine the right user groups to allow for remote management of mobile devices. As in most cases, only full-time employees fall into the category of the user groups, because these devices can contain private and highly sensitive data, it is important they can be remotely managed to allow for locking, tracking, and deleting of data when reported to be lost or reportedly stolen. The apparent reason for this is to restrict an intruder from accessing the device. Respondent two (2) reported the following:

*“Yes, it is important. By controlling and protecting the data and configuration settings of all mobile devices in a network, MDM can reduce support costs and business risks. An MDM intends to optimise the functionality and security of a mobile communications network while minimizing cost and downtime. With mobile devices becoming ubiquitous and applications flooding the market, mobile monitoring is growing in importance. Microsoft helps us test and monitor the delivery of our mobile content, applications, and services.”*

Most modern versions of network operating software (Mac and Windows) have inbuilt security features which can be used to uphold a list of approved devices. This is achieved through a registration procedure whereby the device is accessible and listed on the network. If a device gets misplaced or an employee leaves, the device can be removed/blocked from the list of registered devices. Respondent fourteen (14) had the following to say:

*“It makes our device management more efficient and allows our IT department to reduce risk with fast, automated setup and maintenance of your mobile fleet. Also, by combining mobile device management with the other features, we have a convenient way to manage multiple types of devices from a single web-based console.”*

Understanding that all MDM solutions market the same basic functionalities, deciding on which MDM software to go for should not be based off technical requirements only but also to be balanced by the non-technical necessities of information security (policies and procedures). Respondent Six (6) stressed the importance of a device system management software in an organisation's BYOD policy as seen below:

*“I say it is important. Our MDM service allows us to integrate our existing email setup to be easily integrated with the MDM environment. Almost all MDM products support easy integration with Exchange Server (2003/2007/2010), Office365, Lotus Notes, BlackBerry Enterprise Server (BES) and others. This provides the flexibility of configuring email over the air. Employees frequently copy attachments downloaded from corporate email to their devices and then misuse it. MDM can restrict or disable clipboard usage into or out of the secure*

*container, restrict the forwarding of attachments to external domains, or prevent saving attachments on SD card. This ensures corporate data is secure.”*

Still, on the same issue of importance, respondent eight (8) had the following to say:

*“Mobile device management software allows distribution of applications, data and configuration settings and patches for such devices. Ideally, MDM software allows our IT Manager to oversee mobile devices as easily as desktop computers and provides optimal performance for employees. MDM tools should include application management, file synchronization and sharing, data security tools, and support for either a corporate-owned or personally owned device.”*

Additionally, on the same issue of importance, respondent thirteen (13) had the following to say:

*“Today's IT service management solutions need to account for mobile devices and on-the-go employees. This means you need solid mobile device management software that lets employees be more productive by using their preferred devices while keeping the network safe and secure, as we have done. It is important.”*

Furthermore, a majority of the MDM software has a centralised administration panel that describes basic organisation-wide settings on how to monitor mobile device usage and also enforcing entry-level security functionalities. With regards to which user group can or cannot access specific services, organisations are encouraged to make use of the basic settings that come with the MDM software. Respondents ten (10) had the following to report:

*“The built-in Mobile Device Management (MDM) for Office 365 helps us secure and manage our employees' mobile devices like iPhones, iPads, Androids, and Windows phones. We can create and manage device security policies, remotely wipe a device, and view detailed device reports. Device management is part of our Security & Compliance draft.”*

Another respondent, (12) had the following to say on the same issue:

*“Our Mobile device management from AT&T helps the organisation manage our entire fleet of mobile devices and endpoints while reducing security and compliance risks. It provides visibility into our diverse mobile inventory, enabling us to provision, manage, and help secure specific business data and applications being accessed by employees.”*

### **4.3.3 Policy Review**

Every policy document should comprise of processes and a timetable for its periodic review. This

segment describes a formal procedure for the evaluation and modification of an organisation a BYOD strategy in-order to safeguard that users always have strategies that simulate the organisation's current technological requirements.

Organisations are not only expected to publish a list of devices and platform they would support for employees to use, but they would also need to regularly update this list as we understand that the device and platform landscape is bound to change frequently.

Respondents were asked to explain how frequent a BYOD policy gets reviewed within their organisation. Twenty-eight per cent of the respondents stated that it is important to update the list of supported devices and operating systems, and a list of device recommendation and purchasing guidelines. According to respondent four (4):

*"Like all policy before this, it is important for policies to be reviewed as business needs evolve. We have decided to do this yearly as to all our policies before this. I think it is important; it allows room for additions or subtractions depending on the challenges and opportunities the policy might be exposed to."*

Similarly, respondent six (6) also stated that:

*"I do understand the requirements for a BYOD policy should regularly be reviewed; we have tasked the IT department with making sure our policy development is updated as these device architecture changes, preferably a year gap."*

Organisations are expected to continuously update their policies regarding the authorised use of a mobile device within their environment. This review draws strength from the fact that technology continuously changes. It is recommended to have this policy reviewed at least once a year. The objective is to allow for the provision of solutions to reported problems in the previous year or as foreseen. All relevant stakeholders are to be consulted before refining the policy. This would allow for fewer red-flags and also ensure that requirements are met. Respondent seven (7) stated that:

*"This risk assessment and mobile policy should be regularly updated, as hardware and software change."*

Respondent eight (8) also reported that:

*"Documentation and system processes are the keys to relinquishing control over your data. Not only do we create a full policy and share it regularly with our staff, but it is also enforced and understood at every level. It will live as an ever-changing document, so we keep it live on something like a Wiki where other live documents live and update it when technology changes."*

#### 4.3.4 Limitations of Liability

This segment proposes an overall declaration of disclaimers for which an organisation can absolve themselves of any liability as a result of an individual employee using the company's assets or equipment for illegal activities. In other words, if the said individual employee act against the interest of the company as specified in its policy with regards to the use of its assets, the organisation is not answerable for these actions, presuming that the abuse of trust is not aided by the organisation.

Respondents were asked questions on what measures they put in place to safeguard the organization from the limitation of liability that could arise from either an employee's illegal usage of their devices within the organisation or an employee's violation of the BYOD policy. Some respondents were of the opinion that supports the need to understand the various data security assumptions that come with BYOD implementation, as organisations are expected to know that by welcoming these devices, they may be compromising both their intellectual assets and their overall security. Respondent six (6) had the following to say:

*“Besides the technical challenges that may come from BYOD implementation, security and privacy are part of the risks that come with BYOD. Technical risks here could include how to allow users to connect to the Wi-Fi, how to allow them to access network resources like shared files or printers. Security risks in this context affect both the organisation and employees in different ways. We should worry about the possible local exposure, data leakage, data loss, and prevention against jailbroken devices while the employees are more concerned about the privacy and confidentiality of their data when using the network. So, you see, it is overwhelming if we do not plan against these assumptions before implementing a policy like the one you discussed.”*

Proprietorship should be an important dimension for setting policy guidelines. As a result, corporate and personal mobile artefacts (smartphones and tablets) will have unique sets of rules for security, privacy and application distribution. The change from corporate devices to the personal devices has implications for the retrieval of data when the device is damaged, lost or stolen. To reduce blurred responsibilities for data retrieval in a BYOD environment, organisations must have a distinct policy, showing who owns what data, and whose duty it is to sustain the archives of both the corporate and private data. This policy should also cover responsibility for losses, which have a responsibility to keep this recovery when it is required, and the privacy consequences of such recovery operations. Respondent ten (10) had the following to say:

*“Do have policies that require employees to waive all liabilities in the event that the company remotely locks or wipes a device.”*



As a digital investigation of the personal device as a result of a violation that can be deemed as an incursion of privacy, it is a significant privilege for an organisation to exercise the right to inspect workers' devices at the time of the incident. If the rights are backed up to the arranged policy of the agreed-upon BYOD usage policy, the organisation may face a legal problem and delay when it is necessary to examine the personal data on the device. The present inclination for new and future legislation is beginning to address data breach announcements unless the announcement of specific data protection standards is met. The organisation must express these rules by keeping an active list of mobile artefacts (smartphones and tablets), the data on their security and controls in place to defend these data. Respondent four (4) said:

*“All policies have to be handled by our legal team to see what words to use, how to use them, what works in harmony with existing laws around the workplace. It is important again in any policy formation to have some protection against unforeseen events resulting from the implementation of a policy. The legal bindings make it a policy at the end of the day. So, it plays an important role in any policy document; either to be implemented or not.”*

Likewise, respondent eleven (11) reported the following:

*“Considering our liability. We are a third-party vendor managing information for one or more - or dozens - of clients, we are aware of the civil liability of not having the proper controls and allowing unauthorised criminal access to our client's propriety data. If we unknowingly allow one of your machines to become a bot working for a paid hacker essentially, we can be held liable for real and actual civil damages. At the least, we will lose perhaps hundreds or thousands of staff-hours and be participating and supporting the criminal investigation into how it happened.”*

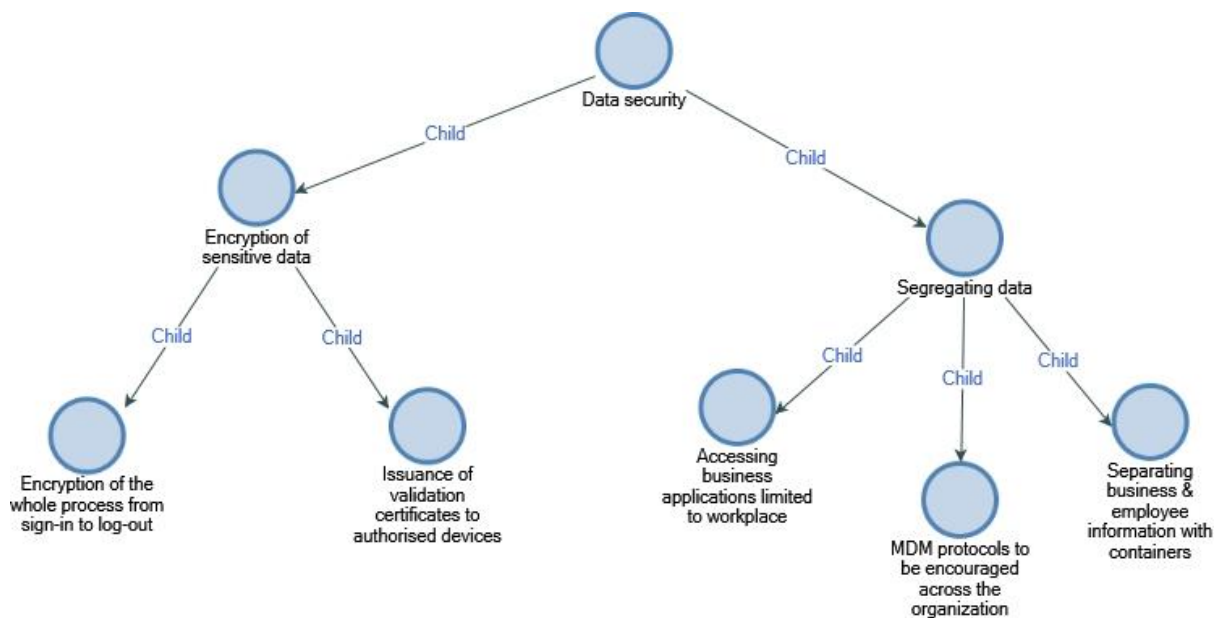
#### **4.4 Security of Data**

From the responses of the interviewees, the factors to consider while developing the BYOD strategy that addresses the security of information available across mobile devices throughout the organisation are characterised into the following themes: segregating data, encrypting data, use of strong passwords, and virtual private network. This is shown in table 4-2 below:

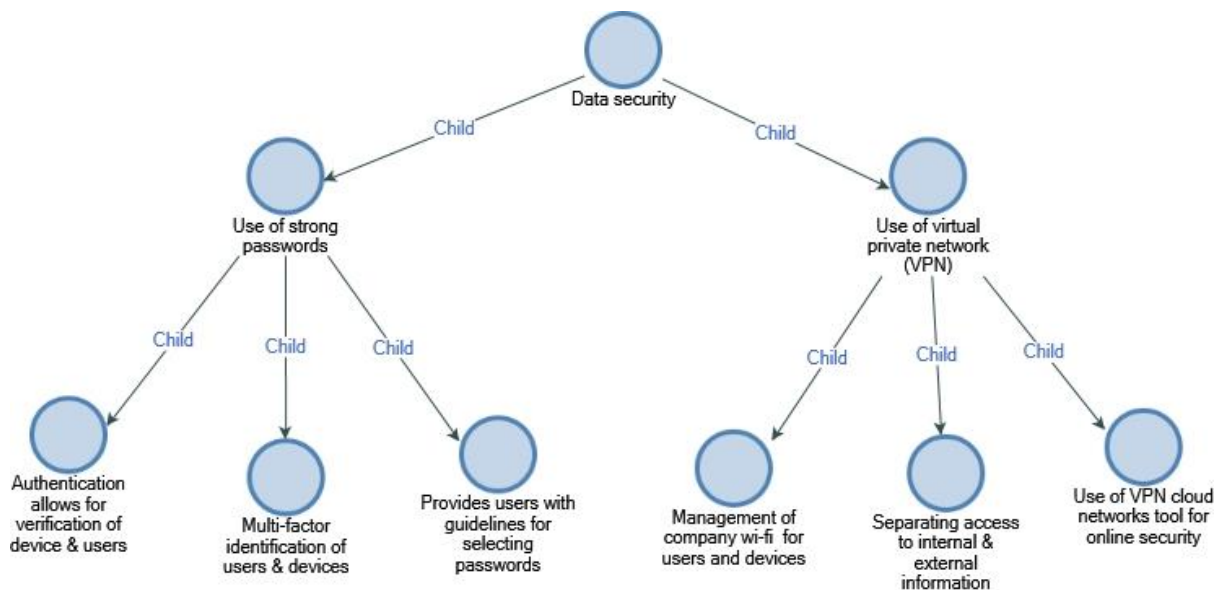
**Table 4-2: Factors that are responsible for safeguarding sensitive information that is accessed on mobile devices throughout an organisation.**

Themes	Frequency of Positive Responses
Segregating Data	7
Registration of Devices	2
Enabling Remote Access to devices	3
Data Encryption	5
Use of a Strong Password for (Device, User, and Container Authentication)	8
Virtual Private Network	6

As further illustrated in Figure 4-4 and Figure 4-5, four sub-themes were identified as an important set of factors based on the frequency of their responses. These sub-themes and their relationship to this study's objectives are presented below.



**Figure 4-4. Security of Data factors and BYOD I**



**Figure 4-5. Security of Data factors and BYOD II**

#### 4.4.1 Segregating Data

As a risk mitigation strategy, the organisation needs to consider separating each device into partitions or compartments; a process called a "container". A separate container is expected to be used for business purposes, and other containers should be used for workers private use.

Containers are to be created to distinctly separate business information from employee information as well as restrict the flow of information amongst each container. Respondent four (4) reported on the following:

*“We only allow these devices to be used as a gateway to access company's data. At no point should this data/information be saved on these personal devices. For example, the email server only allows an IMAP configuration; this allows users only to be able to fetch emails from our mail server and not have these emails stored on the phone which POP3 does. This is one way to design data to be segregated from the user's data. Which was evaluated in our strategy? I would say the thinking is important.”*

Still, on segregating data, respondent six (6) has the following to say:

*“Data security is not necessarily just about keeping the intentionally malicious users at bay; it is also about protecting data against the users who have inadvertently become carriers of the electronic disease. One of the ways we looked at was to have three different layers of security for our network to limit access to sensitive data through different tiers: a public or guest network, a private intranet network and finally, if necessary, a secure and limited access network. The three is being fed from the same internet pipe; they all are behind a properly*

*configured and robust firewall device. The visitorNet provides a convenient place for visitors to have internet access as well as employees who have brought unauthorised devices from home.”*

The selected MDM program must ensure that the organisation efficiently manages and protects the containers containing personal information in any organisation's control or program approved by the company. Although containerization can reduce the risk of privacy and safety concerns; it does not eradicate these risks. Respondent thirteen (13) had this to say:

*“MDM acts as a natural extension to the core risk and security strategy of the enterprise, allowing this organisation to centrally manage and apply policies from the cloud and protect sensitive data on BYOD devices. Similar to any other software being deployed on a large scale, we need to ask the questions is it secure? and what are the risks?”*

Only approved enterprise-approved applications are required to be installed in a business container. An organisations' IT department must be equipped to properly destroy a corporation's container in compliance with the BYOD policy in cases where an employee leaves the company, or there is a report on a missing or stolen device. Another respondent (12), share his opinion as follows:

*“Understanding which data is stored on the device before you deploy a new app. At my company, we only do API calls and store nothing beneath login credentials on the phone. Our cloud serves as intermediate and can regulate or turn off traffic if needed.”*

On the same issue, respondent eleven (11) said:

*“We specify the types of personal data that can be accessed, as well as which devices can be used. The more specific we are, the better – we want to avoid any miscommunication regarding proper usage so that our confidential company data is as secure as possible. It is recommended that antivirus software is installed on personal devices, and technical support is provided to employees on their devices.”*

In the case of a "jailbroken" or "rooted" device, it is common knowledge that the security and privacy controls can be by-passed. To "jailbreak" or "root" a device means waiving both security and privacy features on a mobile artefact, thereby granting the user full management access. This would enable the user to have complete control in deciding on the types of application to install and uninstall apps that he/she would not have been able to. Organisations need to ensure that devices have not been jailbroken into before enabling/supporting them for use within their environment. According to respondent thirteen (13) who said:

*“If a device is brought in that has been connected to other networks and leveraged for other non-work-related tasks, we make sure all of its activity is scanned, filtered and that our network*

*is properly protected from it. We would normally set up a separate Wi-Fi network for BYOD and give it limited access with plenty of filtering.”*

An organisation must have a policy in place to introduce conservation and storage of personal data under its supervision or custody. Ideally, personal data under the management of the organisation should be stored on company networks, or organisations approved devices, not directly on employees' BYOD devices. Using the "thin client" of the organisation can eliminate saving data onto an employee's device. A "thin client" is a technology system that allows a mobile device to act as a read-only station, eliminating the need to store/write data onto the company's servers. This overcomes the fear of data retention since all private data will be made available for read-only purposes via that station, not on the devices entering the office. The storage of personal data on the company's servers will allow the organisation to meet requests for access to custom data as set by applicable laws. Respondent nine (9) stressed that:

*“The focus for keeping data secure shouldn't be on BYOD devices; it should be on applications, no matter which BYOD device is used. We need a cloud security gateway that can enforce corporate policy in cloud applications and data such as with Salesforce, GitHub, and Box as well as homegrown apps. This gets around the problem of pinning our security hopes on device management, which is problematic because people are constantly upgrading, changing their device of choice. That is why we have to secure BYOD usage at the cloud application level.”*

Respondent five, also (5) stated that:

*“Businesses with BYOD policies like ours should instate secure remote access policies, only permitting employees to access corporate data through an encrypted SSL or IPsec connection. As a result of strong encryption algorithms and modern authentication methods, these solutions are a surefire way to keep corporate data safe in a BYOD environment.”*

#### **4.4.2 Data Encryption**

Whitman *et al.* (2013) define encryption as the course of translating an original message into a form that cannot be used by unauthorised persons. That way, anybody without the knowledge on how to convert an encoded message back to its original state will be unable to interpret it.

The science of encryption, known as cryptology, covers two disciplines: cryptography and cryptanalysis. Cryptography - from the Greek words "kryptos," meaning "hidden," and "graphein," meaning "to write" - is the set of processes involved in encoding and decoding messages so that others cannot comprehend them (Whitman *et al.*, 2013). Cryptanalysis - from "analyzein," meaning "to break up"- is the process of decrypting the original message (or plaintext) from an encrypted message (or

ciphertext) without knowing the algorithms and codes used to complete the encryption (Whitman *et al.*, 2013).

Encryption needs should be defined in an organisation's BYOD policy. According to respondents' feedback on encryption requirements, container encryption, device encryption, and the encryption of communication medium between devices and an organisation's network were considered as areas to focus on. Respondent fourteen (14) reported the following:

*“Use encryption on all levels. Your connections should be secured (HTTPS, VPN), your important documents should be encrypted, and devices should have encrypted storage. Even mobiles offer this functionality now.”*

For all encryption solutions, at least an encryption algorithm as per industry standard should be used and must comply with legal requirements to protect sensitive data. Corporations can safeguard their data by using encryption tools, but this technique of defence is as reliable as the actual encryption key. It is possible to encrypt only portions of the data that is stored on the mobile device or the data being transferred over the Internet, or the entire system. The encryption pattern or model adopted should in no way hamper the underlying functions of these mobile devices. To achieve better security, especially with regard to the procedures of logging in, or the transfer of crucial data and information. This can be achieved by applying a more secure protocol to transfer data via certificate authentication and encryption and decryption of data (SSL) and the use of a VPN. Good examples of this technology are bank portals and portals used for handling emails. As reported by respondent six (6) who said:

*“Unencrypted emails, chat and photos present a large risk when stored on a mobile device. When the device is lost, which happens often, then this information could be extracted. Having the right controls (technical and risk management) for your enterprise mobile device infrastructure is key.”*

Respondent five (5) also stated that:

*“One of the biggest offenders to data security is email, especially if companies use a cloud-based service. Sensitive data contained within emails are bounced around multiple servers where copies of this data can be stored. Utilizing an encrypted email client is a cost-effective way of reducing the risk of a data breach via email.”*

Certificates are used to validate a user's identity when trying to access corporate portals. Respondents confirmed that they are trying to safeguard their data using strong access codes and verification, as dictated by standards widely adopted in the IT industry. Respondent thirteen (13) stated that:

*“Our policy absolutely mandates that any device that connects to or holds company data be encrypted at the disk level.”*

Respondent twelve (12) also stressed that:

*“To guarantee that a data-protection strategy is in place for work emails to ensure that all sensitive data is encrypted, proper controls are in place to permit access to that data, and that the policy is consistently tested and audited for effectiveness in preventing data-loss from both external and internal threats.”*

#### **4.4.3 Use of a Strong Password for (Device, User, and Container Authentication)**

Green (2007) describes "*authentication*" as the process of confirming an applicant's identity details through ensuring that the person requesting access is the individual it asserts to be. Distinct users may reveal a personal identification number (PIN) or a passcode to validate their identities to a computer system. After the identity of a user is valid, a process called authorisation defines what the user (whether a person or a computer) has been explicitly and correctly authorised by the proper authority to do, such as access, modify, or delete the contents of an information asset (Green, 2007). An example of authorisation is the activation and use of access control lists and authorisation groups in a networking background.

Another example is a database authorisation structure to confirm that the user of an application is authorised for precise functions, such as reading, writing, creating, and deleting. Valid authorisation and authentication are crucial to guarantee effective safety management for accountability purposes. The following paragraphs touch on device, container and user authentication as authentication areas that should be considered as acknowledged by the respondents.

**Device authentication:** If the BYOD device can connect to a corporate network, such connections must be made using an appropriate remote access method, such as a VPN. Organisations must ensure that each device is adequately verified and reliable before granting access to the network. As reported by respondent seven (7):

*“The idea here is to make sure that the devices connecting to the network with more sensitive data are authorised to do so and meet some standard of authentication as well as virus, malware and spyware prevention and protection. The most secure data is kept extremely limited and not accessible to employee devices. It should only be accessible through two-step authentication measures and should be user limited, IP restricted (if possible) and only available from behind secure VPN connections.”*

Similarly, respondent thirteen (13) also stated that:

*“We enforced good device security. By this, I mean good passwords for access to devices (mobiles, notebooks, and tablets), use of antimalware systems and following standard security practices like ensuring that our OS and critical applications are up-to-date.”*

**Container authentication:** This allows IT division to limit admission to its corporate container to only authorised workers. By checking the integrity of corporate containers, organisations can reduce the release of personal information, and the risk of unauthorised access. According to respondent three (3):

*“By mandating using more than a single factor for authentication, we can be assured that an employee's device has not simply fallen into the wrong hands with a cached password granting the device holder access to our sensitive data.”*

Respondent four (4) also said:

*“It is an important factor in data security. We have evolved into a two-factor authentication which double checks against access to our data internally. Whenever the discussion around security comes up, I think you would agree that passwords are the basic checklist to have in place. However, a strong one is a must-have.”*

**User Authentication:** By adopting MDM software, the use of a secure password can be enforced on all devices that connect to the corporate network. The BYOD device must be set to necessitate each user to identify himself/herself before gaining access to the device with a secure passcode or other approved forms of verification as approved by the organisations' IT division. Although users can choose their pin codes or passwords, central management and coordination of the process by the organisation can be adopted to company policies. As reported by respondent thirteen (13):

*“We enforced the use of antivirus/antimalware software so that when a device connects to our network, it is scanned for having this type of software before it allows a full connection to our network. Lastly, it requires strong passwords and multilevel access control. Gone are the days of P@ssword1 and similar passwords. Passphrases like I l1k3 4urre k@tz can be implemented, and once a user leaves a specific folder location (say like company financials) and attempts to access other data (say like human resources), yet another password (not the same) can be used. Seems like quite a bit, but single sign-on passwords are what have gotten many others in hot water.”*

Users should be provided with guidelines for password selection and maintenance, and the organisation should undertake a periodic review to ensure effective user authentication is in place as required. As a safeguard, BYOD users could be authenticated using multifactor authentication. For example, with two-factor identification, this can involve something that a BYOD user knows (such as a password) and



something that the BYOD user has (such as a token, public-key certificate, or biometric). According to respondent ten (10):

*“The easiest way to solve this common security threat is to ensure that employees use strong passwords using a password management application - ideally one that utilises two-factor authentication as an extra layer of security. This simple step can provide a cost-effective proactive solution to one of the easiest layers for hackers to compromise - the password. We recommend users do not use family or pet names, parts of their Identity number, their employee number, or their phone number as their password combination.”*

Mobile apps that process personal information from the corporate container could also be configured to require separate user authentication. As reported by respondent nine (9) who opined that:

*“A PIN or passphrase must be used to access the device. A good rule of thumb is to require that passwords be at least ten characters long and contain at least one letter, one number, and one special character. If the system allows case-sensitive passwords (or requires them), then at least one uppercase and one lowercase letter should be used as well.”*

Additionally, applications should end a user's session in the event of idleness and should only allow users to re-authenticate themselves before continuing their use. Applications that allow users to be signed on for an un-predefined period should be removed or rendered inoperative. Respondent fourteen (14) said:

*“Applying password enforcement. Although it is quite unpopular, there isn't anything better for service access than strong passwords that are changed from time to time.”*

#### **4.4.4 Virtual Private Network**

A virtual private network is a private, protected network operated over a public and unreliable network. It keeps the details of the network messages concealed from viewers who may have access to public traffic. Using the VPN tunnelling approach, an individual or organisation can set up a network linking on the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to distribute the data safely and securely. Most Microsoft Server software has inbuilt VPN capabilities; comprising Windows Server 2003 and later versions, and client support for VPN services is included in most modern Windows clients (such as Windows 7 and Windows 8). While genuinely secluded network services can cost hundreds of thousands of Rands to rent, configure, and sustain, a VPN can be established for much less.

Most companies and other organisations create virtual private networks that open the direct relationships between their portable devices and their company information systems or networks. This

technology works on the belief of creating a channel between virtual private network applications on mobile devices and virtual private network servers located in corporate information systems. Verification between mobile devices and the network system is done using a certificate - Login is provided after the user's identity has been verified (username, password, and security questions). As reported by respondent four (4) who opined that:

*“We created a bridge between what you can access internally and what you should access externally. Access controls in the form of firewall, IP blocker, virtual networks form our default network configuration. We are just extending that to be part of the BYOD strategy we are formulating. It is important there is a bridge between the private networks and devices.”*

Respondent eight (8) also said:

*“We give the least amount of access to the least number of users. This means that a salesperson should not have access to HR files since there is no reason for them to have it. Because if the sales person's device gets compromised, the attacker will not have access to sensitive files from another department.”*

Most mobile devices have inbuilt support for VPN capabilities to allow for the provision of a secure tunnel to an organisation's network, protecting data in motion. Most VPN solutions offer granular access that is founded on user roles, amongst other factors. Machine verification can determine the device and user, and a wide array of constraints of the device itself, such as whether anti-virus, anti-spyware or private firewalls are allowed, or if the device's operating system is one of the acceptable versions, patches and service packs. If you want to monitor access to additional built-in or certification by third parties, you can add an additional layer of protection, especially in case of lost or stolen mobile devices.

Many of the enterprise-class VPN devices also offer a mobile client, which can support secure access for native business apps (such as Exchange, Oracle, SAP and the like) and HTML5 apps via a secure browser. These apps can be authorised for precise users and automatically connected to the users' devices from an integrated enterprise app store. There is a great deal of control over the apps themselves, as well – mobile VPN connections can be facilitated per application, and applications can be authorised per user. As reported by respondent five (5) who opined that:

*“Instating secure remote access policies, only permitting employees to access corporate data through an encrypted SSL or IPsec connection. As a result of strong encryption algorithms and modern authentication methods, these solutions are a surefire way to keep our corporate data safe in a BYOD environment.”*

Respondent six (6) also said:

*“Our firm uses a VPN cloud-network tool that uses secure servers for online security and privacy. This allows us to secure their data, including any app data, by replacing personal employee IP addresses with a generic IP address. This helps to block out any hackers that may attempt to steal company information through employee devices.”*

Often in a bid to provide security against data leakage, most mobile clients have inbuilt secure container whose sole responsibility is to store all data associated with the organisation. These secure containers are designed to be remotely erased in cases where the device has been reported stolen or missing, which offer greater security for the organisation data against allowing intruders to have access. As reported by respondent seven (7) who opined that:

*“The idea here is to make sure that the devices connecting to the network with more sensitive data are authorised to do so and meet some standard of authentication as well as virus, malware and spyware prevention and protection. The most secure data is kept extremely limited and not accessible to employee devices. It should only be accessible through two-step authentication measures and should be user limited, IP restricted (if possible) and only available from behind secure VPN connections.”*

Also, other VPNs offer many remote desktop access features that allow the user to use the phone and use their familiar desktop environment the way they are used to do. This competence dramatically diminishes training and support needs when employees access and use the desktop interface they use every day on a computer or laptop provided by the company.

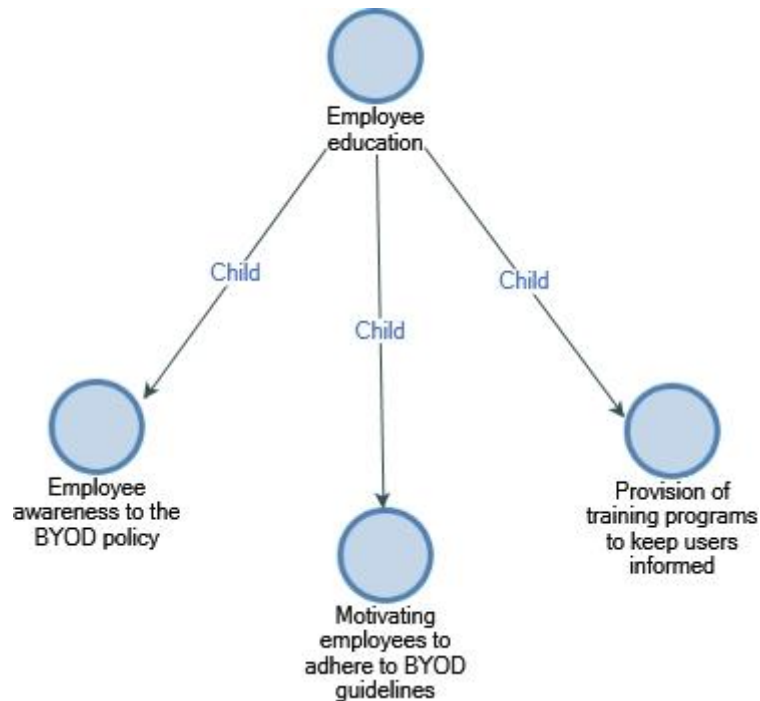
VPN utilities can also provide a virtual portal that can be personalised by the type of device that people use to access the network, for example, a virtual mobile portal can be developed to be responsive on devices with a smaller screen to facilitate interaction and communication. As reported by respondent twelve (12) who opined that:

*“The IT department manages our company Wi-Fi well. Ideally, we have 4 Wi-Fi's: corporate, employees, visitors and devices. Since every device will be connected to the network, this is very important.”*

#### **4.5 Employee Education**

Factors to consider when developing an employee education strategy that can include safety standards and regulations for mobile devices used throughout an organisation are categorised into Employee Awareness, Employee Motivation, Employee Education and Training.

As illustrated in Figure 4-6, three sub-themes were identified as an important set of factors based on the frequency of their responses. These sub-themes and their relationship to this study's objectives are briefly explained below.



**Figure 4-6. Employee Education factors and BYOD**

Maintaining a proper BYOD environment necessitates that the policy is incorporated into all human resources activities, including hiring, training, promotion and termination practices. Next, employers should inform employees which devices, operating systems, and apps will be maintained on employees' devices, analyzing the rationale for these decisions is vital. A convenient time is during employee orientation. At this critical time, employees are educated on a wide variety of organisational policies and on the expectations that the organisation has for its employees. Because employees should have no preconceived notions or established methods of behaviour at that point, they are more likely to be receptive to this instruction. This openness is balanced against their lack of familiarity with the systems and their jobs, so any issues that they might have questions about will not have arisen yet.

According to Respondent five (5) who stated that:

*“BYOD in our case works for both parties; the employees drove the need for us to have a strategy formulated in the first place. So, therefore, the employees being aware of it and how they can benefit from the policy is very important.”*

IT divisions' discussions on company access and security should comprise how workers access the corporate network from the company Wi-Fi as well as from the standard Wi-Fi networks. Managers should also deliberate on what ensues in the case of lost or stolen devices.

Regarding data ownership, business leaders should deliberate on the use of corporate/personal e-mail, social networks, corporate/personal contacts, and the company data on the employee-owned device. BYOD training for employees should embrace how to properly log in to the corporate network, as well as how to accept software, applications, and updates.

Employees must also be told about the penalties of breaching the accountabilities to comply with the policies and the outcomes of breaching the corporate policies. One method of guaranteeing that policies are read and understood by general users is to provide training on those policies. This strategy allows users to ask questions and receive specific direction, and it allows the organisation to gather the required letters of compliance. These general users also need training on the technical details of how to do their jobs securely, including good security practices, password management, specific access controls, and violation reporting.

According to respondent ten (10) who stated that:

*“We do provide security awareness training about the risks associated with mobile devices and the importance of timely reporting of lost or stolen devices.”*

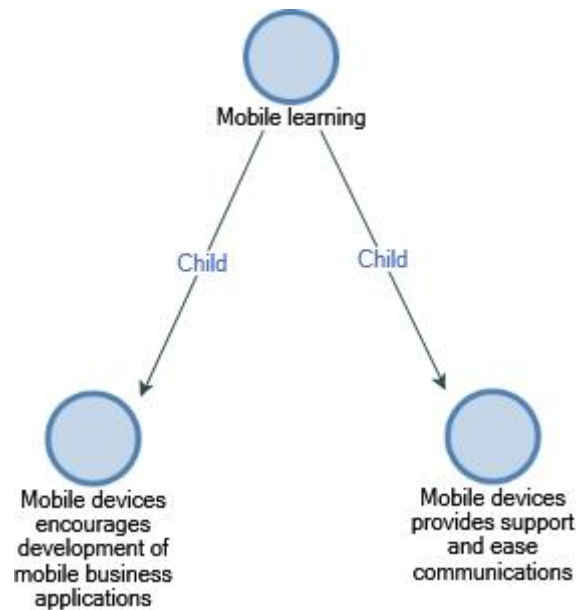
Likewise, respondent eight (8) also stated that:

*“Documentation and system processes are the keys to relinquishing control over your data. Not only do we create a full policy and share it regularly with our staff, but it is also enforced and understood at every level. It will live as an ever-changing document, so we keep it live on something like a Wiki where other live documents live and update it when technology changes.”*

## **4.6 Mobile Learning**

The responses of the various participants on the identifiable standard set of factors that should be considered when designing an approach that addresses the use of portable devices for learning are categorised into Ease of communication and Micro-app Development.

As illustrated in Figure 4-7, two sub-themes were identified as an important set of factors based on the frequency of their responses. These sub-themes and their relationship to this study's objectives are briefly explained below.



**Figure 4-7 Mobile Learning in organisations and BYOD**

Using BYOD as a study tool gives mobile learning providers the ability to create good quality products. These products can be consumed faster on a mobile device to offer flexible learning onboarding and learning pace. One thing to take note of is a user's relationship with his or her device. Users are far more likely to spend enough time interacting with learning applications and tools on a device they are familiar with as compared to devices forced upon them. As a powerful training tool for learning, BYOD opens the market for mobile learning suppliers to take care of the needs of individual learning organisations.

Traditionally the limited budget of the smaller organisations means getting fewer training materials than their multinational colleagues. It is still in its early stages to determine if BYOD plays a crucial role in levelling the playing field; but arguably, it positively gives small-to-medium organisations the needed boost.

According to respondent four (4) also stated that:

*“I do not think this is important too. The relevance is there, but the importance is not something we have thought of yet. Communication tools like Slack and Jira do have native mobile applications that can be easily installed on mobile devices, but we do not expect employees to replace these tools used on a desktop with a mobile version. This allows us to respect their privacy outside of the work environment. In another case, we have some chat groups on WhatsApp that were only being accessed on mobile devices until WhatsApp recently developed desktop clients that do the same thing.”*

In a BYOD culture, it is expected that employees have access to a mobile device, mostly personally-owned, this allows an organisation to save cost on procuring these devices, to begin with. By doing this, organisations only have to worry about filling these devices with applications and content. Contents referred to includes skills-based content and crowd-sourced content.

#### **4.7 Summary of Research Findings.**

This section explains in summary how the findings from the empirical phase addressed each research question and ultimately achieving the corresponding research objective. This summary is discussed below:

##### **To Determine the Various Factors When Drafting/Creating a Policy for the Acceptable and Prohibited Use of Personally Owned Mobile Device in the Workplace.**

The purpose of this objective was to determine the relevant factors best to consider when adopting a policy for the suitable and prohibited use of a personally owned portable handheld device. Based on the responses gathered from respondents, the factors that determine the appropriate policy to be put in place for the adoption of a BYOD strategy are authorised usage, systems management, policy review and statement of purpose.

##### **To Determine Appropriate Factors Allowed to Ensure an Organisation's Data is Secure While Enabling the Use of Personally Owned Mobile Handheld Devices in the Workplace**

The purpose of this objective was to determine relevant factors to be considered to adequately safeguard an organisation's data while enabling the use of an individually owned portable handheld device. From the findings gathered, participants opined that factors such as: segregating data, data encryption, use of a strong password for the following types of authentication (device, user, and container), and Virtual Private Network were important factors to be considered. A small number of participants (2) also believed that factors such as registering of the device and enabling remote access to the device should also be taken into considering when securing an organisation's data or information.

##### **To Ascertain the Right Methods to Raising Employee Awareness of Safety Standards and Regulations When Using a Personally Owned Mobile Device in the Workplace**

This objective looks at how employees are both aware and mindful of best safety practices and values when it comes to using a mobile device within an organisation. Participants believed that adequate training should be provided to employees on the various policies and regulations of the organisation.

Training enables an employee to ask questions they need more information about. By doing this, they receive guidance and instructions on the various policies and regulations within the organisation.

### **To Determine the Right Modality to Be Incorporated When Designing Learning Experiences That Cater to the Unique Technical Elements of Mobile Devices in the Workplace**

The final objective of this study was to determine the right modality for consideration when planning learning experiences that cater to the unique practical elements of portable devices. The modalities highlighted were: Ease of communication and Micro-app Development. Organisations are increasingly adopting the mobile device platform as the preferred learning delivery channel, even though the choices are hinged on budget availability. Small and Medium organisations are leveraging on these available devices to provide learning experiences for their employees.

## **4.8 Conclusion**

This section ascertains that all the research questions in this study were addressed. The sub-section addressed each research objective in-order to verify that all research objectives were met. The different policies that should be considered when developing a BYOD policy were discussed. Similarly, this section also addressed the security measures to be put in place for adopting a BYOD strategy.

Furthermore, it also discussed mobile learning and employee education, as seen in each section in this chapter. This chapter proposed a conceptual framework that was used to evaluate and document the set of factors IT managers need to consider when adopting a strategy that addresses the use of individually owned BYOD (smartphones and tablets) within the organisation. The next chapter concludes the study by providing limitations, recommendation, and suggestions for future research.



## **CHAPTER 5: SUMMARY, RECOMMENDATIONS AND CONCLUSION**

### **5.1 Introduction**

This chapter's objective is to provide a comprehensive summary of the previous chapters. It also presents recommendations and conclusion based on the findings of the study. This study entailed an investigation of the factors that IT managers need to consider when devising a strategy for the use of individually owned BYOD artefacts such as smartphones and electronic tablets into an organisation. The overall objective of the study was to document a set of factors that need to be given priority consideration before employees are allowed the privilege of bringing personal computing devices into the confines of the organisational IT infrastructure. A non-probability sampling method using a purposive sampling technique was adopted to identify the participants of this study. Furthermore, this study elicited information by conducting interviews amongst fourteen senior executives with standard titles such as CIO, CEO, Director, and Managing Director operating small to medium-sized organisations in South Africa that either considers IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. These organisations drive the company's revenue through the values generated by the adoption of IT as a business enabler.

Data collected from the study were analysed using a thematic analysis. Themes were generated based on the conceptual framework adopted by this study, and the information provided by participants during the interviewing process. This chapter begins, however, with a summary of findings from the researcher's engagement with reviewed literature and the conceptual framework adopted for this study, which justifies the present study. The chapter, then, makes some recommendation on the study based on the findings and ends with a conclusion.

### **5.2 Summary of Dissertation**

This study was aimed at identifying the factors that IT managers need to consider when implementing strategies for the use of personal devices (smartphones and tablets) within an organisation. The focus is on the working environment, with the objective to create a set of factors to take into account when adopting a BYOD strategy for the whole organisation. The research questions that this study was focused on investigating are restated below:

- What factors are to be taken into account when developing a policy for the satisfactory use and prohibited use of personal portable handheld devices in the workplace?
- What factors should be reviewed to ensure an organisation's data is secure while allowing the use of individually owned devices by employees in the workplace?

- What approach must be taken into account in order to raise employee awareness of safety benchmarks and pronouncements in the use of portable personal devices in the workplace?
- What modality should be factored in when designing a work learning experience that satisfies the unique technical elements of portable devices in the workplace?

This dissertation comprises of five chapters, including this chapter. The summary of each chapter is presented below.

**Chapter 1:** This chapter starts with an introduction and background to the study. It also describes the research problem, research objectives and research questions that the study aims to answer. It further gave justification and significance for carrying out this research, including a brief description of the research methodology employed in the research.

**Chapter 2:** This chapter presents a comprehensive review of the literature on a BYOD strategy. Several definitions were given with a description of key concepts that made up the research study. The chapter also elaborates on various works of literature on BYOD policy, BYOD and data security, BYOD and employee education, BYOD and mobile learning. It further included the conceptual framework that would go on to guide the empirical phase of the study, including the process with which the framework was validated.

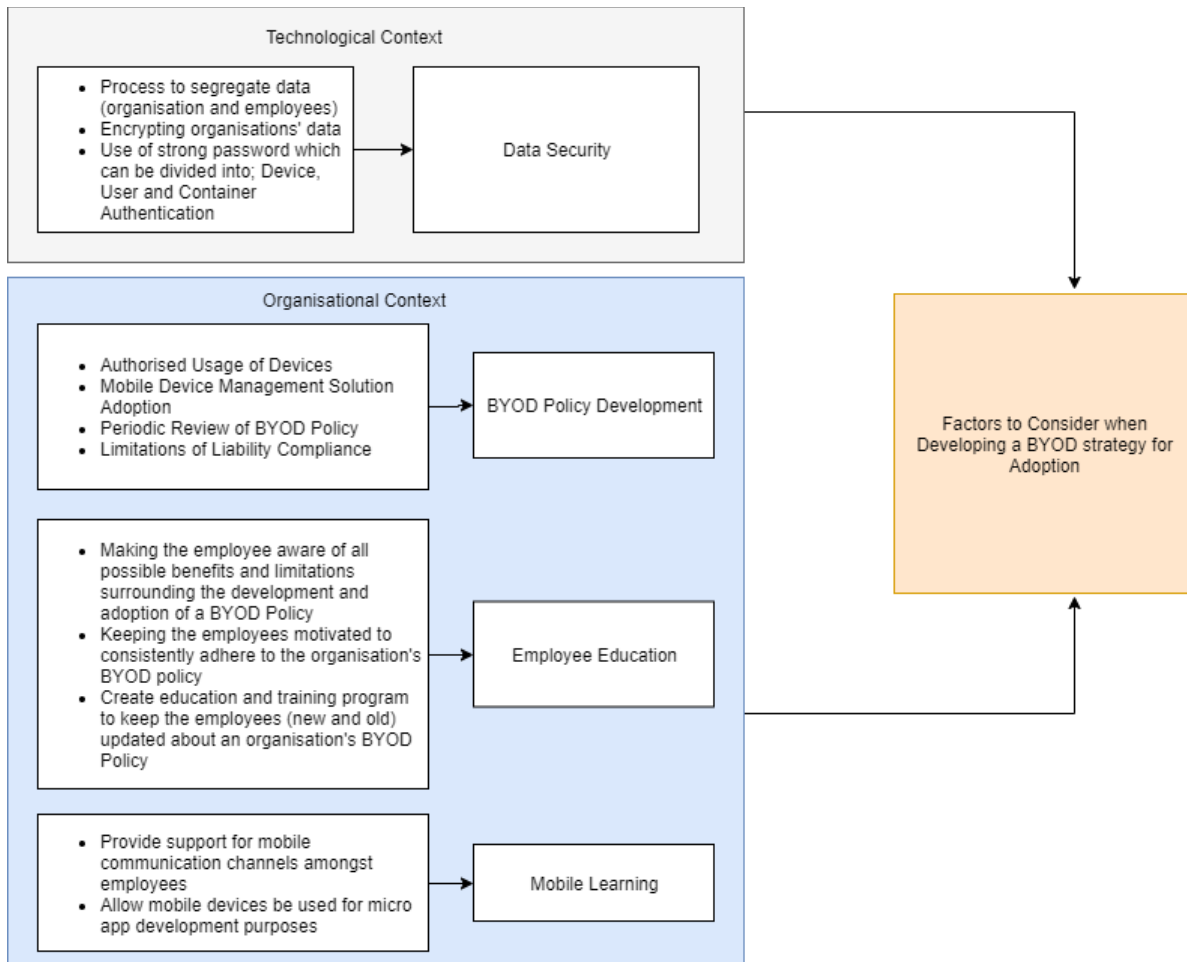
**Chapter 3:** This chapter outlines the research methodology adopted in the study. It also presents the method of data collection, the data collection instrument, the sampled population, and the sampling method used in the study. The chapter also outlays the data analysis technique adopted in the dissertation.

**Chapter 4:** In this chapter, data obtained during the empirical phase was extensively analysed and discussed using the thematic analysis technique. In order to accurately present the research findings, a conceptual framework was used in tandem with the literature to adequately address the objectives of this research study by identifying various factors that IT managers need to consider when implementing strategies for the use of personally owned mobile artefacts (smartphones and tablets) within an organisation.

**Chapter 5:** This chapter gives a summary of the key conclusions obtained during the analyses of data and discussions of findings in the fourth chapter. It also concludes by recommending areas in the study that require future research work.

### 5.3 Summary of Research Findings

This section summarises the findings from the study in relation to the conceptual framework and research objectives, and this is represented in the diagram below. Each construct in the diagram below directs each research question and its corresponding objective in this study.



**Figure 5-1: Adjusted Conceptual Framework concerning Factors for consideration when Developing BYOD Strategy Model Integration within an Organisation**

The diagram above represents the conceptual framework that was adopted for this study. As seen above, the primary construct highlighted guided each research question posed in this study. The themes derived from each of the constructs which have been highlighted above have been identified by respondents as important factors to take into consideration when developing an organisation-wide BYOD strategy.

**Research objective one: To determine the various factors to be considered when drafting/creating a policy for the acceptable and prohibited use of personally owned portable devices in the workplace.**

The findings revealed that planning a BYOD IT policy is the starting point in the development of an organisation-wide BYOD strategy. Some of the participants agreed that in a BYOD culture, an organisation's IT policy needs to ensure that its network is secured, and its IT division should have control over this data, which is more precise than the traditional IT policy. Also, the BYOD policy must be designed from all users' perspective. Further conclusions revealed that the IT department must guarantee that users are educated on the vulnerability and limitation of using their devices at work. From the data gathered, authorised usage, systems management, policy review and statement of purpose were the four main factors identified that should provide detailed and targeted information when designing a BYOD IT Policy, see Figure 5.1 above.

**Research objective two: To appropriate factors to be taken to ensure an organisation's data is secure while consenting to the utilisation of individually owned portable electronic devices in the workplace**

The findings showed that most of the participants believe that there is an amount of data security risk that comes with allowing the use of employee-owned devices within the organisation. In the adoption of BYOD strategy, an organisation's competitive advantage which was promised by the adoption of mobility can be lost if the devices entering the workplace are not giving the needed protection against data security threats. Further findings revealed that participants identify security breach from the possible loss and theft of a mobile device as one of their first concerns regarding the use of these devices within the organisation. From the findings gathered, participants opined that factors such as: segregating data, data encryption, use of a strong password for the following types of authentication (device, user, and container), and Virtual Private Network were important factors to be considered by an IT division to ensure that data is adequately secured in a BYOD environment, see Figure 5.1 above.

**Research objective three: To ascertain the right approach to be taken into account in order to raise employee awareness of safety benchmarks and pronouncements when utilizing personally owned portable devices in the workplace.**

The key findings for this objective revealed that educating users to play a crucial role in harmonizing both BYOD strategy, BYOD implementation, and adherence. The use of personally-owned mobile devices on an organisation's network raises the need for IT division to educate users to help protect data of both parties. Additionally, most participants agree that periodic training programs on both the recommended and inappropriate use of mobile devices within the organisation should be provided to

all employees. Majority of the respondents also agree that training should be recommended as part of an organisation's initial hiring orientation, or orientation to an organisation's resources. It should also be offered at consistent times throughout a business calendar year, should an employee demand that their device is approved for use on an organisation's network.

**Research objective four: To determine the right modality that can be incorporated when drafting work learning experiences that satisfies the exceptional technical elements of portable devices in the workplace**

The data collected revealed that most participants were not aware of the need to cater to mobile learning experiences when framing a BYOD strategy. The extent to which participants considered this as a factor in the formulation of a BYOD strategy varied. Only a few claimed to be familiar with how they can leverage mobile devices to incorporate learning into employees work routine, others felt that they had no available data to consider the factor as important as the incorporation of learning into work routines while leveraging on mobile devices is still in the early stages as the design of learning with mobile devices is in the early stages. Additionally, participants were stable with the presentation/definition of a set of characteristics to be considered when leveraging mobile devices platform to develop learning experiences to incorporate into work routines within an organisation. There are two factors, namely Ease of communication and Micro-app Development as identified by respondents.

#### **5.4 Recommendations of Research Findings**

From the findings and responses of the sampled executives, the following recommendations are drawn:

To ensure adequate development of a BYOD strategy across an organisation, the organisation should be willing to put all needed resources in place to ensure that employees are presented with a company owned mobile device for use. The management of the organisation should also try to ensure that all the employees have declared and registered any personal devices that they have.

Several policy guidelines need to be in place when developing a BYOD strategy. A complete full usage guideline needs to specify which devices are allowed and how employees will be notified that their devices satisfy the authorised criteria. The policy should deliver a list of compliant and preferred vendors for sourcing devices and license for core applications required. Moreover, a clear statement needs to detail how employee-owned devices will be configured, which applications will be buoyed, and the type of support that will be provided. The guidelines also need to determine which devices are appraised on an ongoing basis, particularly as new devices, platforms, and operating systems emerge

and employee expectations evolve. At the same time, the four identified sections that direct the needed factors to consider when adopting a BYOD policy are presented in Table 5-1 below.

**Table 5-1: Detailed Direction for Developing a BYOD Policy**

Policy Section	Content Description
Authorised Usage	This section talks on what type of technology and tools can be used within the organisation and who the authorised users are. As reported by Emery (2012), an organisation must have a defined list of authorised users (employees, vendors, and partners), mobile devices, and technology to allow in the workplace. Furthermore, as reported by the respondents, this section describes the potential risks to an invasion of privacy and personal data that the authorised users agreed to before using a personal mobile device within an organisation.
Systems Management	This segment emphasises the employees' relationship with systems management. According to respondents, an organisation should have detailed instructions regarding the use of e-mail and electronic documents and storage of those documents. One example would see a section that talks on enforcing power-on authentication for a user's mobile device before use on an organisation's network.
Policy review	In this section, the IT governance team defines a method for the evaluation and modification of the organisation's BYOD strategy to safeguard users, and that its strategy provides accommodation for current technologies requirement. Majority of the respondents agreed with Emery (2012), who reported that an organisation is expected to continuously update their policies regarding the authorised use of mobile devices within their environment.
Limitations of Liability	This section recommends an overall declaration of disclaimers for which an organisation can absolve themselves of any liability as a result of an individual employee using the company's assets or equipment for illegal activities. For example, if an employee act against the interest of the company as specified in its policy with regards to the use of its assets, the organisation is not answerable for these actions, presuming that the organisation does not aid the abuse of trust.

Data security is one of the main priorities when developing a BYOD strategy. It is essential to determine which corporate applications can be accessed from an employee-owned device. IT division needs to be

able to manage device and access policies, preferably from a single point of control. The IT division can ensure security policies relating to VPN, anti-virus software, activation of personal firewalls or use of encryption are enforced, and that in the event of a device being lost or stolen, IT division can remotely wipe organisation data. Organisations not only need to consider the value of their data and the risk of losing it, but also the potential compliance and reputation implications. From the findings of this study, respondents identified four key factors that an IT division can consider ensuring that an organisation's data is secure in a BYOD culture, see Table 5-2 below.

**Table 5-2: Detailed Guide to Ensure the Security of Data in a BYOD organisation**

Security Safeguard	Description
Segregating Data	It is essential for IT division to design the organisation's data in a way that it is segregated from employees' data. The respondents shared a similar view with Wittman (2012), who reported that an organisation could save itself a lot of resources in the event of litigation and any compliance-related audits. One of the recommended ways of segregating data is to allow for the provision of storage space to enable employees back up work-related data. Furthermore, most of the respondents agree with Harris (2012) reported that there must be clear communication around employees' saving their personal data in these containers.
Data Encryption	An organisation should be proactive in using encryption techniques and software to carefully encrypt either the whole information system or specific segments of data on devices accessing its data.
Use of a Strong Password for (Device, User, and Container Authentication)	Strong passwords are to be requested from devices and users trying to access an organisation data container. This simple authentication procedure proves to be an adequate safeguard against limiting unknown access to an organisation's resource such as wireless network, and information system.
Virtual Private Network	A VPN works on the principle of creating a private channel between two devices. Majority of the VPNs creates an established link between a VPN software on a mobile device and the VPN server located within an

	organisation (Emery, 2012). The link between the device and information system needs to be verified as well as the identity of the user before granting remote access.
--	--

Individuals must give wholly informed and unambiguous consent for an organisation to access and process their data. On the other hand, organisations processing sensitive personal data must take adequate technical and organisational measures to protect that data. At a minimum, in the world of BYOD, this means that devices must support encryption, either on the device or the communications channel, and the organisation must enforce a strong password policy.

The use of personally-owned portable devices within an organisation raises a needed demand on IT divisions to properly educate their users on processes to follow to help protect data for both the organisation and the user. From the findings of this study, respondents identified three key factors that an IT division can consider ensuring that an organisation raises employee awareness of safety standards and regulations when using a personally owned mobile device, see Table 5-3 below.

**Table 5-3: How to raise employee education on safety standards when using a personal device within the organisation**

<b>Employee Education Context</b>	<b>Description</b>
Employee Motivation	Apart from relevant departments raising employee awareness and training them on the safety standards to adhere to when using their devices within the organisation, they need to understand that employees need to be motivated internally to want to adhere to these policies. It is recommended to make users understand that the policy looks after their well-being as well as that of the organisation, while also making them aware of the ethical and moral expectations of the need for the policy and the adverse effects of breaching these policies to make them more likely to follow the instructions.
Employee Awareness	Organisations are recommended to adequately sensitise users of the need to be conscious of how they use their devices within the organisation. The constant flow of information about this raises the safety awareness of users as it becomes easy to be motivated to adhere to the security guidelines required of them.
Employee Training	Organisations are recommended to provide training programs on both the appropriate and inappropriate use of mobile



	<p>devices of employees within the organisation. This should cover topics like privacy settings, creating a password, how to share information across social media. It is recommended to provide these training programs as part of a new staff hiring process or can be scheduled as part of an in-flight activity.</p>
--	--

In the process of drawing up factors directly responsible for the design of learning experiences on mobile devices within an organisation, the focus should be on the functionality features of these devices and how it can be used to support the learning experiences for employees. From the findings of this study, respondents identified two key factors that an IT division can consider when designing learning experiences in a BYOD culture, see Table 5-4 below.

**Table 5-4: Details to Designing Learning Experiences in a BYOD Culture**

<b>Mobile Learning Context</b>	<b>Description</b>
Ease of communication	<p>This section focuses on how the mobile device differs from a desktop or even mainframe computers because of its potentials to using the wireless network to access the Internet, and how employees can leverage the mobile device to allow them to interact with colleagues within the workplace. Most of the respondents agree with Motiwalla (2007) who reported that this functionality gives employees the potential for instant and sometimes constant feedback by allowing them to interact with colleagues, clients, and access organisation materials from anywhere they have wireless connectivity.</p>
Micro-app Development.	<p>The development of custom mobile apps has been made possible through the release and use of SDKs. This enables the IT department to roll out custom apps quickly to speed up the productivity of users within an organisation. An example is where an organisation allows the use of mobile devices to streamline its employee attendance system; this app replaces the manual attendance taking system as it is task-specific.</p>

## **5.5 Limitations and Recommendations for Further Research**

Even though this research has provided insights on the set of features needed to be deliberated when developing an organisation-wide BYOD strategy for adoption, some restrictions are recognised below after which suggestions for future research were made.

### **5.5.1 Sampling Procedure**

The non-probability sampling procedure in the form of purposive sampling, also termed judgmental technique was used in identifying executives operating small to medium-sized businesses, and this is under the non-probability sampling method. The purposive sampling method is the process where a researcher selects samples based on specific characteristics or traits exhibited, which is a bit of a misnomer; there is no intended bias in purposive sampling. However, as a result of a lack of random sampling, purposive sampling is sometimes open to selection bias and error. Even if the researcher tried to eliminate selection bias to the best of his/her ability, it could be problematic to defend his/her choices for participants. Therefore, the researcher cannot generalise the outcome of this study's results to the entire population. Although this sampling method was providing the necessary insights to the study's questions, it is suggested that other sampling methods could have been adopted.

### **5.5.2 Exclusions**

This study is not focused on a BYOD strategy for specific organisations but rather on the general factors involved in planning a BYOD strategy to support an organisation's strategic objectives. This study does not seek to recommend a specific implementation for an organisation's data networking infrastructure, but rather on how an organisation's data network can be designed to improve data security factors relative to the use of personally owned mobile handheld devices by its employees.

### **5.5.3 Future Research**

The focus of this study was to identify a set of factors to be considered when developing an organisation-wide BYOD strategy for adoption. The research setting for this study is the eThekweni Municipal Region of South-Africa. The target population comprises of organisations in eThekweni Municipal Region, South Africa that either consider IT to be mission-critical because the business relies on it to operate or where IT services is the fundamental thing that the business does. These organisations drive the company's revenue through the values generated by the adoption of IT as a business enabler. Further studies should be carried out involving other types of organisations; educational institutions and professional associations as all these industries are faced with different experiences and challenges in dealing with the rise of BYOD.

Furthermore, other organisation types such as voluntary organisations, non-profit organisations, non-governmental organisations and trade unions could be involved where the use of general IT devices is limited. This study was only limited to responses from respondents in the eThekweni Municipal Region. Future research can have responses from study sites outside of this area.

Furthermore, BYOD affords end users the freedom to collaborate and be productive anytime, anywhere. Along with these benefits, however, BYOD has a highly disruptive impact on IT, shifting the balance of power from centralised IT decision making to a decentralised end-user base. Therefore, there is a need to investigate the impact of BYOD on employees' productivity and organisation performance.

Additionally, many enterprises have not taken time to assess how user behaviour with personal devices impacts their infrastructure needs. Although the first sign of consumerisation may be the need to support new device types, this is just the beginning. Companies must consider not only how they will offer secure access to corporate data and applications but also how they will protect that information once it is on an employee-owned device.

Furthermore, there is a need to carry out similar research in other developing African nations to carefully establish whether the set of factors to be considered when developing a BYOD strategy for an organisation's acceptance are a country-based set of factors, or it is an industry-based set of factors. The objective is to add more literature to the already existing literature about BYOD, especially in the local context where research about the subject matter is either limited or do not exist.

## **5.6 Conclusion**

The main objective of this study was to highlight important factors that IT managers need to consider when implementing strategies for using personal devices (smartphones and tablet PCs) within an organisation. A conceptual framework was used to guide the course of the study. Using the primary constructs of the conceptual model, it was deduced that the key factors that IT managers need to consider when implementing strategies for using personal devices within an organisation should be framed into a selected set of four more significant categories of factors. These four broader categories of factors are policy development, data security, employee education and mobile work-learning.

One part of the findings of this study was to determine the best factors to consider when adopting a policy for the suitable and forbidden use of a personally owned portable handheld device. Based on the responses gathered from respondents, the factors that determine the appropriate policy to be put in place for the adoption of a BYOD strategy are authorised usage, systems management, policy review and

statement of purpose. Another objective was to determine relevant factors to be considered to adequately safeguard an organisation's data while enabling the use of an individually owned mobile device. From the findings gathered, participants opined that factors such as: segregating data, data encryption, use of a strong password for the following types of authentication (device, user, and container), and using a virtual private network are important factors to be considered. Another objective was to provide a set of factors that addresses how employees are both aware and mindful of best safety practices and values when it comes to using a mobile device within an organisation; factors involved here include employee motivation and employee awareness and training. The final objective was to determine the right modality for consideration when planning learning experiences that cater to the unique practical elements of portable devices at work. Factors identified from the findings of the study include ease of communication and micro-app development.

## REFERENCES

- A. Harris, M. & P. Patten, K. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22, 97-114.
- Akour, H. (2009). *Determinants of mobile learning acceptance: an empirical investigation in higher education*. Oklahoma State University.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26, 276-289.
- Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29, 432-445.
- Alzahrani, J. G. & Ghinea, G. (2012). Evaluating the impact of interactivity issues on e-learning effectiveness. *2012 International Conference on Information Technology Based Higher Education and Training (ITHET)*. Institute of Electrical & Electronics Engineers (IEEE).
- Attwell, G., Cook, J. & Ravenscroft, A. (2009). Appropriating technologies for contextual knowledge: Mobile personal learning environments. *Best practices for the knowledge society. Knowledge, learning, development and technology for all*. Springer.
- Battaglia, M. (2008). Encyclopedia of survey research methods. *Publication date*.
- Beaulieu, M.-D., Samson, L., Rocher, G., Rioux, M., Boucher, L. & Del Grande, C. (2009). Investigating the barriers to teaching family physicians' and specialists' collaboration in the training environment: a qualitative study. *BMC medical education*, 9, 31.
- Bhattacharjee, A. (2012). Social science research: principles, methods, and practices.
- Bigalk, D. & Bigalk, D. (2006). Lernförderliche Arbeitsplätze. Verständnis und Anforderungen. IN LOROFF, C., MANSKI, K., WALTER MATTAUCH & SCHMIDT, M.(Eds.) *Arbeitsprozessorientierte Weiterbildung. Lernprozesse gestalten, Kompetenzen entwickeln Bielefeld, W. Bertelsmann Verlag*.
- Brandly, T. (2011). Pros and cons of bringing your own device to work. *PC World, December 20 2011. Disponible en [http://www.pcworld.com/article/246760/pros\\_and\\_cons\\_of\\_byod\\_bring\\_your\\_own\\_device\\_.html](http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html)*.
- Brandt, E., Hillgren, P.-A. & Björqvinnsson, E. B. (2004). Self-produced video to augment peer-to-peer learning. *Learning with mobile devices: Research and development: A book of papers*, 27-34.
- Braun, V., Clarke, V. J. I. j. o. q. s. o. h. & well-being (2014). What can “thematic analysis” offer health and wellbeing researchers? 9.
- Braun, V. & Clarke, V. J. Q. r. i. p. (2006). Using thematic analysis in psychology. 3, 77-101.
- Brenda, P., DeBruin, D., Bartels, D., Chambers, E. & Kahn, J. (2003). *A guide to research ethics*, UNIVERSITY OF MINNESOTA CENTER FOR BIOETHICS.
- Bughin, J., Chui, M. & Manyika, J. (2013). Ten IT-enabled business trends for the decade ahead. *McKinsey Quarterly*, 13.
- Burt, J. (2011). BYOD trend pressures corporate networks. *eweek*, 28, 30-31.
- Chen, Y., Liu, Z., Jakubowski, M. H. & Yacobi, Y. (2011). Data protection for a mobile device. Google Patents.
- Chinnathambi, V., Rajasekar, S. & Philominathan, K. (2013). Research methodology. *India: Tamilnada*.
- Clarke, V. & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist*, 26, 120-123.
- Crook, S. K. (2013). BYOD Security Tips. *Bring Your Own Devices (BYOD) Survival Guide*. Informa UK Limited.

- Cummins, M., Johnson, L. & Adams, S. (2012). *The NMC horizon report: 2012 higher education edition*, The New Media Consortium.
- David, B., Yin, C. & Chalon, R. (Year) Published. Contextual mobile learning for appliance mastery. IADIS International Conference Mobile Learning, 2007.
- De Vaus, D. A. & de Vaus, D. (2001). *Research design in social research*, Sage.
- Devers, K. J. & Frankel, R. M. (2000). Study design in qualitative research--2: Sampling and data collection strategies. *Education for health*, 13, 263.
- Edelheit, D., Stuckey, D., Sage, J., Singh, S. & Cuneo, M. (2012). Bring your own device agility through consistent delivery. Retrieved August, 7, 2012.
- Emery, S. (2012). Factors for consideration when developing a bring your own device (BYOD) strategy in higher education.
- Eugene, M. (2014). *BYOD Catching SA Companies By Surprise* [Online]. Available: <http://saitnews.co.za/opinion/catching-companies-surprise/> [Accessed].
- EY (2013). Bring Your Own Device: Security and Risk Considerations for Your Mobile Device Program. In: YOUNG, E. (ed.) *Insights on Governance, Risk, and Compliance Collection*.
- Felstead, A., Fuller, A., Jewson, N. & Unwin, L. (2009). *Improving working as learning*, Routledge.
- Fereday, J. & Muir-Cochrane, E. J. I. j. o. q. m. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. 5, 80-92.
- Fogarty, K. (2010). Cloud Computing: Today's Four Favorite Flavors. *Explained. CIO. the CIO site* [http://www.cio.com/article/598918/Cloud\\_Computing\\_Today\\_s\\_Four\\_Favorite\\_Flavors\\_Explained](http://www.cio.com/article/598918/Cloud_Computing_Today_s_Four_Favorite_Flavors_Explained) ([http://www.cio.com/article/598918/Cloud\\_Computing\\_Today\\_s\\_Four\\_Favorite\\_Flavors\\_Explained](http://www.cio.com/article/598918/Cloud_Computing_Today_s_Four_Favorite_Flavors_Explained)) (Accessed: 31 July 2010).
- Garlati, C. (2011). Trend micro consumerization report 2011. Retrieved on May, 1, 2015.
- Gartner (2018). Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017. In: GARTNER (ed.).
- Gill, J. & Johnson, P. (2010). *Research methods for managers*, Sage.
- Golafshani, N. (2003a). Understanding reliability and validity in qualitative research. *The qualitative report*, 8, 597-606.
- Golafshani, N. (2003b). Understanding reliability and validity in qualitative research. *The qualitative report*, 8, 597-606.
- Goucher, W. (2009). The challenge of security awareness training. *Computer Fraud & Security*, 2009, 15-16.
- Gray, D. E. (2013). *Doing research in the real world*, Sage.
- Green, A. (2007). Management of security policies for mobile devices. *Proceedings of the 4th annual conference on Information security curriculum development - InfoSecCD '07*. Association for Computing Machinery (ACM).
- Greener, S. & Wakefield, C. (2015). Developing confidence in the use of digital tools in teaching. *Electronic Journal of E-Learning*, 13, 260-267.
- Guarte, J. M. & Barrios, E. B. (2006). Estimation under purposive sampling. *Communications in Statistics—Simulation and Computation*®, 35, 277-284.
- Guest, G., Bunce, A. & Johnson, L. J. F. m. (2006). How many interviews are enough? An experiment with data saturation and variability. 18, 59-82.
- Hagen, J., Albrechtsen, E. & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Info Mngmnt & Comp Security*, 19, 140-154.

- Hardwig, T. (2006). Worauf kommt es bei der betrieblichen Gestaltung lernförderlicher Rahmenbedingungen eigentlich an. *IN LOROFF, C., MANSKI, K., WALTER MATTAUCH & SCHMIDT, M.(Eds.) Arbeitsprozessorientierte Weiterbildung. Lernprozesse gestalten, Kompetenzen entwickeln. Bielefeld, W. Bertelsmann Verlag.*
- Harris, C. (2012). IT executive and CEO survey final report: Mobile consumerization trends and perceptions. *Trend Micro (2012). Enterprise readiness of consumer mobile platforms. Retrieved October, 26, 2012.*
- Härtel, M., Gerwin, W. & Kupfer, F. (2007). Der Beitrag arbeitsplatznaher elektronischer Informations-und Lernsysteme für berufliche Qualifizierungsprozesse. *Abschlussbericht zum Forschungsprojekt.*
- Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47, 154-165.*
- Hulley, S. B., Cummings, S. R., Browner, W. S., Grady, D. G. & Newman, T. B. (2013). *Designing clinical research*, Lippincott Williams & Wilkins.
- ICT-Policy-Review. (2013). *Information Technology, Supplementary Insights* [Online]. Available: <http://www.doc.gov.za/key-programmes/ict-policy-review.html> [Accessed].
- IT-Online. (2014). *BYOD security lags in SA* [Online]. Available: <https://it-online.co.za/2014/08/22/byod-security-lags-in-sa/> [Accessed].
- IT-Online. (2016). *Can BYOD sharpen the line between work and home?* [Online]. Available: <https://it-online.co.za/2016/09/30/can-byod-sharpen-the-line-between-work-and-home/> [Accessed].
- Joppe, M. (2000). The Research process.
- Kellogg, S., Booth, S. & Oliver, K. (2014). A social network perspective on peer supported learning in MOOCs for educators. *The International Review of Research in Open and Distributed Learning, 15.*
- Kerlinger, F. N. J. P. R. (1970). A social attitude scale: Evidence on reliability and validity. *26, 379-383.*
- Kim, P. (2010). *Measuring the effectiveness of information security training: a comparative analysis of computer-based training and instructor-based training*, ProQuest LLC. 789 East Eisenhower Parkway, PO Box 1346, Ann Arbor, MI 48106.
- Kim, R. (2011). The iPhone effect: How Apple's phone changed everything. Gigaom. Retrieved 2016-02-30, from <https://gigaom.com/2011/06/29/the-iphone-effect-how-applesphone-changed-everything>.
- Kinash, S. (2006). Paradigms, methodology & methods. *Bond University. Australia.*
- Koeberl, P., Li, J., Rajan, A., Vishik, C. & Wójcik, M. (2012). Consumerization: Consequences of Fuzzy Work-Home Boundaries. *ISSE 2011 Securing Electronic Business Processes*. Springer Science + Business Media.
- Kothari, C. R. (2011). *Research methodology: methods and techniques*, New Age International.
- Kukulska-Hulme, A. & Traxler, J. (2005). Mobile teaching and learning. *Mobile learning-a handbook for educators and trainers, 25-44.*
- Lacey, A. & Luff, D. (2001). *Qualitative data analysis*, Trent Focus Sheffield.
- Lakshman, M., Sinha, L., Biswas, M., Charles, M. & Arora, N. (2000). Quantitative vs qualitative research methods. *The Indian Journal of Pediatrics, 67, 369-377.*
- Lincoln, Y. S. J. T. B. E. o. S. (1985). Naturalistic inquiry.
- Loroff, C. (2006). *Arbeitsprozessorientierte Weiterbildung: Lernprozesse gestalten, Kompetenzen entwickeln*, Bertelsmann.

- Lunsford, T. R. & Lunsford, B. R. (1995). The Research Sample, Part I: Sampling. *JPO: Journal of Prosthetics and Orthotics*, 7, 17A.
- Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*, 2012, 14-17.
- Markelj, B. & Bernik, I. (2013). MOBILE DEVICES AND EFFECTIVE INFORMATION SECURITY. *IIASS*, 6.
- Markelj, B. & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *journal of information security and applications*, 20, 84-89.
- Marshak, R. (2006). Cisco Systems. Patricia Seybold Group (PSG).
- Marshall, C. & Rossman, G. B. (2014). *Designing qualitative research*, Sage publications.
- Mazzoni, E. & Gaffuri, P. (2009). Monitoring Activity in E-Learning: A Quantitative Model Based on Web. *Monitoring and Assessment in Online Collaborative Environments: Emergent Computational Technologies for E-Learning Support: Emergent Computational Technologies for E-Learning Support*, 111.
- Mictseta (2012). The Media, Information and Communication Technologies Sector Education and Training Authority Sector Skills Plan 2013–2018.
- Morehouse, R. E. & Maykut, P. (2002). *Beginning qualitative research: A philosophical and practical guide*, Routledge.
- Moschella, D. (2005). What the Consumerization of IT means to your business, ten messages for CXOs. *Retrieved August*, 8, 2012.
- Motiwalla, L. F. (2007). Mobile learning: A framework and evaluation. *Computers & Education*, 49, 581-596.
- Mwenemeru, H. K., Omwenga, V. O. & Kenya, K. (2014). Towards the adoption of bring\_your\_own\_device concept in an organization. *International Journal of Social Sciences and Entrepreneurship*, 1, 534-546.
- Networks, A. (2012). *The Aruba Mobile Virtual Enterprise: A Mobility-Centric Network Access Architecture*.
- Norris, C. A. & Soloway, E. (2011). Learning and schooling in the age of mobilism. *Educational Technology*, 51, 3.
- Oliveira, T. & Martins, M. F. J. E. J. o. I. S. E. (2011). Literature review of information technology adoption models at firm level. 14, 110.
- Omwenga, V. O. & Mwenemeru, H. K. (2015). Towards the adoption of bring\_your\_own\_device concept in an organization.
- Ortbach, K., Walter, N. & Öksüz, A. (Year) Published. Are You Ready to Lose Control? A Theory on the Role of Trust and Risk Perception on Bring-Your-Own-Device Policy and Information System Service Quality. 2015.
- Pachler, N., Pimmer, C. & Seipold, J. (2011). *Work-based mobile learning: concepts and cases*, Peter Lang.
- Pasanen, J. (2003). Corporate mobile learning. *Mobile Learning*, 115-123.
- Patton, M. Q. (1990). *Qualitative evaluation and research methods*, SAGE Publications, inc.
- Peraković, D., Husnjak, S. & Remenar, V. (Year) Published. Research of security threats in the use of modern terminal devices. 23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability, 2012.
- Pimmer, C., Pachler, N. & Attwell, G. (2010). Towards work-based mobile learning: what we can learn from the fields of work-based learning and mobile learning. *International journal of mobile and blended learning*, 2, 1-18.
- Pirttiahho, P., Holm, J.-M., Paalanen, H. & Thorström, T. (Year) Published. Etaitava-Mobile Tool for On-the-Job Learning. IADIS international Mobile Learning Conference, Lisbon, 2007. 218-222.



- Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26, 229-237.
- Radicati. (2016). *Email Market, 2016–2020 – Executive Summary* [Online]. Palo Alto. Available: <https://www.radicati.com/wp/wp.../Email-Market-2016–2020-Executive-Summary.pdf> [Accessed].
- Rajasekar, S., Philominathan, P. & Chinnathambi, V. (2006). Research methodology. *arXiv preprint physics/0601009*.
- SaInfo. (2013). *ICT and electronics in South Africa* [Online]. Available: <http://www.southafrica.info/business/economy/sectors/ict-overview.htm#ixzz2h8sDQxhY> [Accessed].
- Saksida, M. (2008). Preprečite uhajanje podatkov iz omrežja. *Pridobljeno*, 17, 2011.
- Saldaña, J. (2015). *The coding manual for qualitative researchers*, Sage.
- Saunders, Lewis, P. & Thornhill, A. (2012). *Research Methods for Business Students*.
- Saunders & Tosey, P. (2013). *The Layers of research design*.
- Sekaran, U. & Bougie, R. (2013). *Research methods for business : A skill- building approach*, United Kingdom, John Wiley & Sons
- Sen, P. K. (2012). Consumerization of information technology: Drivers, benefits and challenges for New Zealand corporates.
- Sharples, M., Taylor, J. & Vavoula, G. (Year) Published. Towards a theory of mobile learning. *Proceedings of mLearn*, 2005. 1-9.
- Shenton, A. K. J. E. f. i. (2004). Strategies for ensuring trustworthiness in qualitative research projects. 22, 63-75.
- Singh, N. (2012). BYOD genie is out of the bottle–“Devil or angel”. *Journal of Business Management & Social Sciences Research*, 1, 1-12.
- Siponen, M. & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.
- Souppaya, M. & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST special publication*, 800, 124.
- Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, 24, 124-133.
- Stewart, G. & Lacey, D. (2012). Death by a thousand facts. *Info Mngmnt & Comp Security*, 20, 29-38.
- Strauss, A. & Corbin, J. (1998). *Basics of qualitative research techniques*, Sage publications Thousand Oaks, CA.
- Swanson, K. (2008). Merrill Lynch: Bullish on mobile learning. *Chief Learning Officer*, 7, 54-59.
- Theoharidou, M., Mylonas, A. & Gritzalis, D. (Year) Published. A risk assessment method for smartphones. *IFIP International Information Security Conference*, 2012. Springer, 443-456.
- Thomson, G. (2012). BYOD: enabling the chaos. *Network Security*, 2012, 5-8.
- Tornatzky, L. G., Fleischer, M. & Chakrabarti, A. K. (1990). *Processes of technological innovation*, Lexington books.
- Traxler, J. (2007). Defining, Discussing and Evaluating Mobile Learning: The moving finger writes and having writ. *The International Review of Research in Open and Distributed Learning*, 8.
- Trend-Micro (2012). Enterprise readiness of consumer mobile platforms. *Retrieved July*, 12, 2012.
- Ullman, E. (2013). BYOD strategies: Strategies for K-12 technology leaders. *Technology & Learning*, 32, 34-37.
- Van Wyk, B. (2012). Research design and methods Part I.

- Vodafone (2013). Vodafone Global M2M Services and Strategy. *In: VODAFONE (ed.)*.
- Von Koschembahr, C. & Sagrott, S. (2005). The future of learning at IBM. *Mobile Learning: A Handbook for Educators and Trainers*, 164.
- Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, 10, 69-80.
- Wallen, N. E. & Fraenkel, J. R. (2013). *Educational research: A guide to the process*, Routledge.
- Weekes, S. (2008). Mobile learning-is anyone using it. Retrieved.
- Whitman, M. & Mattord, H. (2013). *Management of information security*, Nelson Education.
- Wittman, A. (2011). BYOD? First get serious about data security. *Information Week*, 1316, 46.
- World-Wide-Worx (2012). Internet Access in South Africa 2012 report. South Africa.
- Yang, K., Subramanian, N., Qiao, D. & Zhang, W. (2011). A Pervasive Mobile Device Protection System. *Iowa State University*.
- Yarmey, K. (2015). Student Information Literacy in the Mobile Environment. *The Role of the Library*. Informa UK Limited.

# APPENDICES

## Appendix A: Ethical Clearance Letter



15 September 2016

Mr Solomon Oluwaseun Omokehinde (214577345)  
School of Management, IT & Governance  
Westville Campus

Dear Mr Omokehinde,

Protocol reference number: **HSS/1394/016M**

Project title: Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) strategy for adoption

### Full Approval – Expedited Application

In response to your application received on 24 August 2016, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

**PLEASE NOTE:** Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. The reafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Dr Shamilla Naidoo (Deputy Chair)

/ms

Cc Supervisor: Mr Ashley Marimuthu  
Cc Academic Leader Research: Professor Brian McArthur  
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee

Dr Shanuka Singh (Chair)

Westville Campus, Govan Mbeki Building

Postal Address: Private Bag X64001, Durban 4000

Telephone: +27 (0) 31 266 2387/0350-1557 Facsimile: +27 (0) 31 260 4608 Email: [hrhsep@ukzn.ac.za](mailto:hrhsep@ukzn.ac.za) / [hrhsec@ukzn.ac.za](mailto:hrhsec@ukzn.ac.za) / [hrhsc@ukzn.ac.za](mailto:hrhsc@ukzn.ac.za)

Website: [www.ukzn.ac.za](http://www.ukzn.ac.za)



100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Durbanville Howick College Medunsa Pietermaritzburg Westville

## **Appendix B: Informed Consent Document**

### **UNIVERSITY OF KWAZULU-NATAL SCHOOL OF MANAGEMENT, IT & GOVERNANCE**

#### **MCom (Research) IS&T Research Project**

Ms. M Snyman

Humanities and Social Science Ethics (HSSREC) Research Office,  
Govan Mbeki Building, Westville Campus, Private Bag X54001, Durban 4000

Tel: 031 260 8350      Email: Snymanm@ukzn.ac.za

**Researcher:** Solomon Oluwaseun Omokehinde (0837344661)

**Supervisor:** Mr. M Marimuthu

Dear Respondent,

My name is **Solomon Oluwaseun Omokehinde**. I am a **MCom (Research)** student in the Discipline of Information Systems and Technology, in the School of Management, Information Technology and Governance at the University of KwaZulu-Natal Westville campus Durban South Africa. I hereby invite you to please participate in a research project titled “**FACTORS TO CONSIDER WHEN DEVELOPING AN ORGANISATION-WIDE BRING YOUR OWN DEVICE (BYOD) STRATEGY FOR ADOPTION**”.

The aims of this study are:

1. To determine the various factors to be considered when developing a policy for the acceptable and prohibited uses of personally owned mobile handheld devices?
2. To determine appropriate factors allowed to ensure an organisation’s data is secure while enabling the use of personally owned mobile handheld devices?
3. To ascertain the right methods for consideration in raising employee awareness of safety standards and regulations when using a personally owned mobile device?
4. To determine the right modality for consideration when designing work experiences that cater for the unique technical elements of mobile devices?

Through your participation I hope to identify the Factors IT leaders should consider when developing an organisation-wide Bring Your Own Device (BYOD) strategy for adoption within organisations in South Africa.

The results of the survey are intended to provide valuable and informed factors needed to successfully develop an organisation-wide BYOD strategy within organisations in South Africa. The study would also be of great help tot South African IT leaders in the field of Information, Communications and technology by providing a BYOD strategy document that would assist in the use of mobile device usage within organisational context.

- Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you will be maintained by the School of Management, IT & Governance, UKZN. The interview is for about 30 minutes

If you have any questions or concerns about the interview schedule questions or about participating in this study, you may contact me or my supervisor at the numbers listed above.

**Please note:**

- The interview would be for about 30 minutes.

**Thank you for your willingness to participate!**

**DECLARATION**

This letter confirms that I ..... (Full names of the participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project of the above student. I also hereby consent / do not consent to have this interview recorded.

I understand that participation in this study is voluntary and there are no penalties should I wish to terminate my participation.

Participants Signature: .....

Date: .....

## Appendix C: Questionnaire

Research Topic: **FACTORS TO CONSIDER WHEN DEVELOPING AN ORGANISATION-WIDE BRING YOUR OWN DEVICE (BYOD) STRATEGY FOR ADOPTION**

M.Com (Research)

Discipline of Information Systems & Technology

School of Management, Information Technology & Governance

University of KwaZulu-Natal (Westville Campus)

**Researcher:** Solomon Omokehinde (0837344661) **Supervisor:** Mr. M Marimuthu

### INTRODUCTION

My name is Solomon Oluwaseun Omokehinde with student number (214577345) from the Discipline of Information Systems and Technology, in the School of Management, IT and Governance at the University of KwaZulu-Natal Westville campus Durban South Africa.

I would like to ask you some questions that are related to the factors IT leaders should consider when developing an organisation-wide Bring Your Own Device (BYOD) strategy for adoption within your organisation. The questions would enable me to gain the required insight and understanding of the various factors identified in relation to mobile policy, data security, employee education and mobile learning.

The information acquired during the interview would shed more light on the pre-identified factors needed for developing a BYOD strategy document within organisations within South Africa. It will also elaborate more on the existing BYOD policy being applied by your organisation.

The following key words would be frequently used during the interview:

BYOD – A term used to refer to the trend of bringing a personally owned mobile device to the workplace for use and connectivity on an organisation's network

Mobile device - A handheld computing device that can be used from multiple locations. Examples include basic phones, portable media players, and smartphones

Mobile Device Management (MDM) – Software designed to securely manage mobile devices used across an enterprise.

Microapp – An application specifically developed and designed for use on a mobile handheld device.

Information Systems – Better described as the combination of the hardware and software systems that support data intensive applications and processes.

Mobile Learning – a learning model that provides ubiquitous, mobile, and anytime access to organisation's resources empowered by mobile technology in its connected or disconnected form.

Smartphone – A fully featured mobile telephone with personal computer-like functionality.

Tablet – A mobile computer integrated into a multi-touch screen and operated by touching the screen rather than using a physical keyboard and mouse.

The interview is for about 30 minutes.

The interview schedule questions are as follows:

### **BYOD Strategy**

1. Does your company currently have a BYOD policy regarding the use of employee owned devices in accessing the company network?
  - a. If yes, what is the status of your company's BYOD policy regarding the use of employee owned devices in accessing the company network?
  
2. From your understanding for the need of a BYOD strategy, can you give a brief description of the perceived importance and benefit of having one implemented in your organisation in relation to the following
  - a. Making corporate data more secure?
  - b. Integration into Overall corporate risk management policy?
  - c. Increased productivity amongst employees?
  - d. Reduced IT cost in my organisation?
  - e. Giving us a competitive advantage over our competitors?

### **BYOD POLICY DEVELOPMENT**

3. If you were given all needed resources to properly develop a BYOD policy for your organisation, how much importance would you place on each of the identified factors in relation to a BYOD policy development:
  - a. The framework should properly describe the security guidelines for mobile devices usage within an organisation?
    - i. If important, could you explain how the security guidelines for mobile devices usage were considered sufficiently in your organisation's BYOD policy?
    - ii. If not important, could you explain why this is not important?
  - b. The framework should properly explain the authorised use of what technology and devices can be used for within an organisation?
    - i. If important, could you explain how the authorised use of mobile device was considered sufficiently in your organisation's BYOD policy?
    - ii. If not important, could you explain why this is not important?

- c. The framework should properly explain the prohibited usage of what technology and devices cannot be used for within an organisation?
  - i. If important, could you explain how the prohibited usage of mobile device was considered sufficiently in your organisation's BYOD policy?
  - ii. If not important, could you explain why this is not important?
- d. The framework should look at a device system management tool that describe rules for employees using mobile devices to ensure they meet certain requirements when using a mobile device, as well as any applications or data contained on the mobile device?
  - i. If important, could you explain how a device system management software/tool was considered sufficiently in your organisation's BYOD policy?
  - ii. If not important, could you explain why this is not important?
- e. The framework should inform users of the penalties involved if they violate the policy, as well as how to report suspected violation of the policy by others within an organisation?
  - i. If important, could you explain how the penalties for violation of policy were considered sufficiently in your organisation's BYOD policy?
  - ii. If not important, could you explain why this is not important?
- f. The framework should inform users of how and when an existing BYOD policy will be reviewed within an organisation?
  - i. If important, could you explain how frequent a policy gets reviewed was considered sufficiently in your organisation's BYOD policy?
  - ii. If not important, could you explain why this is not important?
- g. The framework should ensure that the organisation is not liable in the event an employee willfully violates this policy resulting in any type of criminal or civil penalty?
  - i. If important, could you explain how a legal protection from limitations of liability by employee(s) using a personal mobile device was considered sufficiently in your organisation's BYOD policy?
  - ii. If not important, could you explain why this is not important?

## **DATA SECURITY**

- 4. In its bid to save an organisation a lot of wasted energy in the event of litigation and compliance-related audits. How important is designing an organisation's data to be segregated from user's personal data?
  - a. If important, could you explain how segregating an organisation's data from employee's data was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?



5. In its bid to provide IT department with the ability to track the user's mobile device. How important is the process of registering a device for use on an organisation's network?
  - a. If important, could you explain how registering a device for use on an organisation's network was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
6. Prior to a user's mobile device to being lost or stolen, how important is the need for employee to give access to IT department to enable remote to wipe the data on the mobile device?
  - a. If important, could you explain how enabling remote access to employee mobile device was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
7. Encryption software can be used to encrypt only certain segments of data on a mobile device. How important is the need to implement data encryption shared across information systems in an organisation?
  - a. If important, could you explain how implementing data encryption was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
8. Using a strong password on a mobile device can be a simple yet effective safeguard. How important is the use of strong password a criterion to accessing an organisation's network?
  - a. If important, could you explain how enforcing the usage of strong password was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
9. A VPN functions on the principle of establishing a channel between the virtual private network servers that is located within the organisation's information system. How important is the need to set-up access controls to verify the identity of a user before granting access to a system on the network?
  - a. If important, could you explain how setting up access controls (firewalls, VPNs) was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?

## **EMPLOYEE EDUCATION**

10. How important is the need to educate employees on the purpose for a BYOD policy within an organisation?
  - a. If important, could you explain how educating employees on the need for a policy was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
11. How important is the need to train employees to raise awareness of threats that are facilitated by user negligence or unawareness within an organisation?

- a. If important, could you explain how train employees to raise awareness of threats that are facilitated by user negligence or unawareness were considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
12. How important is the need to encourage and motivate employees to commit to security guidelines and policies within an organisation?
- a. If important, could you explain how encouraging and motivating employees to commit to security guidelines and policies was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?

### **MOBILE LEARNING**

13. Mobile devices could be used for common desktop application utilities, including productivity related microapps. How important is the need for an organisation to allow mobile devices to be used for learning purposes with regards to their roles within an organisation?
- a. If important, could you explain how allowing the use of mobile device to be used for learning purpose was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
14. A wireless mobile device overcomes the limitations of desktop or even laptop computers as they can leverage a wireless carrier's network to access the Internet/Intranet. How important is the need for organisation to allow mobile devices to be used as a communication tool within an organisation?
- a. If important, could you explain how allowing the use of mobile device to be used for communication was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?
15. Mobile device is seen as a way to streamline lengthy business workflow. How important is the need for an organisation to allow microapps to be used as business tools to streamline its workflow?
- a. If important, could you explain how allowing the use of microapps to be used for streamlining business workflow was considered sufficiently in your organisation's BYOD policy?
  - b. If not important, could you explain why this is not important?

## Appendix D: Interview Protocol

According to Stacy and Paige (2012), an interview protocol goes beyond a list of interview questions; it also expands to the procedural level of conducting interviews and often encompasses the script of what the interviewer is expected to say before an interview, the script for what is expected to be said by the interviewer when concluding the interview, cues to help the interviewer collect informed consent, and cues or prompts to guide or remind the interviewer on the kind of data/information he or she is required to collect from the interviewee.

The interview protocol employed in this study is as seen below;

Interview Protocol Title:

Date:

Time:

Location:

Interviewer:

Interviewee(s):

Introductory Speech:

I would like to welcome you and thank you for your participation today. My name is Solomon Oluwaseun Omokehinde and I am a master's student at the University of KwaZulu-Natal Westville Durban and conducting this research in partial fulfilment of the requirements for a Master's degree in Information Systems and Technology. I would like to ask you some questions that are related to the factors IT leaders should consider when developing an organisation-wide Bring Your Own Device (BYOD) strategy for adoption within your organisation. The questions would enable me to gain the required insight and understanding of the various factors identified. The interviews will take about 1 hour for each respondent and will include 15 questions in relation to mobile policy, data security, employee education and mobile learning. The interview is a standardised open-ended one as it would give room for some flexibility when answering the research questions.

I would also want to seek your permission to record this interview using a mobile phone, so that the information conveyed by you would be adequately documented. Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this interview. Confidentiality and

anonymity of records identifying you as a participant will be maintained by the School of Management, IT & Governance UKZN.

I would also like to bring to your attention your written consent to take part in this study. I am the responsible investigator, indicating your participation in this research study: Factors for Consideration When Developing an Organisation-Wide Bring Your Own Device (BYOD) Strategy. We both have signed and dated each copy of the consent letter, indicating that we agree to proceed with this interview. You would be given one copy and the other copy would be kept in a secure location by me.

Thank you.

Do you have any lingering questions/concerns before we start the interview? Then with your consent we will start the interviews.

The interview questions are as follows:

#### **BYOD Strategy**

1. Does your company currently have a BYOD policy regarding the use of employee owned devices in accessing the company network?
  - a. **Probe:** If yes, what is the status of your company's BYOD policy regarding the use of employee owned devices in accessing the company network?

[Researchers comments]

[Reflective notes from the researcher]

2. From your understanding for the need of a BYOD strategy, can you give a brief description of the perceived importance and benefit of having one implemented in your organisation in relation to the following
  - a. Making corporate data more secure?
  - b. Integration into Overall corporate risk management policy?
  - c. Increased productivity amongst employees?
  - d. Reduced IT cost in my organisation?
  - e. Giving us a competitive advantage over our competitors?

[Allow for flexibility]

[Researchers comments]

[Reflective notes from the researcher]

#### **BYOD POLICY DEVELOPMENT**

3. If you were given all needed resources to properly develop a BYOD policy for your organisation, how much importance would you place on each of the identified factors in relation to a BYOD policy development:

a. The framework should properly describe the security guidelines for mobile devices usage within an organisation?

i. **Probe:** If important, could you explain how the security guidelines for mobile devices usage were considered sufficiently in your organisation's BYOD policy?

ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

b. The framework should properly explain the authorised use of what technology and devices can be used for within an organisation?

i. **Probe:** If important, could you explain how the authorised use of mobile device was considered sufficiently in your organisation's BYOD policy?

ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

c. The framework should properly explain the prohibited usage of what technology and devices cannot be used for within an organisation?

i. **Probe:** If important, could you explain how the prohibited usage of mobile device was considered sufficiently in your organisation's BYOD policy?

ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

d. The framework should look at a device system management tool that describe rules for employees using mobile devices to ensure they meet certain requirements when using a mobile device, as well as any applications or data contained on the mobile device?

- i. **Probe:** If important, could you explain how a device system management software/tool was considered sufficiently in your organisation's BYOD policy?
- ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

- e. The framework should inform users of the penalties involved if they violate the policy, as well as how to report suspected violation of the policy by others within an organisation?
  - i. **Probe:** If important, could you explain how the penalties for violation of policy were considered sufficiently in your organisation's BYOD policy?
  - ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

- f. The framework should inform users of how and when an existing BYOD policy will be reviewed within an organisation?
  - i. **Probe:** If important, could you explain how frequent a policy gets reviewed was considered sufficiently in your organisation's BYOD policy?
  - ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

- g. The framework should ensure that the organisation is not liable in the event an employee willfully violates this policy resulting in any type of criminal or civil penalty?
  - i. **Probe:** If important, could you explain how a legal protection from limitations of liability by employee(s) using a personal mobile device was considered sufficiently in your organisation's BYOD policy?
  - ii. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

## DATA SECURITY

4. In its bid to save an organisation a lot of wasted energy in the event of litigation and compliance-related audits. How important is designing an organisation's data to be segregated from user's personal data?
  - a. **Probe:** If important, could you explain how segregating an organisation's data from employee's data was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

5. In its bid to provide IT department with the ability to track the user's mobile device. How important is the process of registering a device for use on an organisation's network?
  - a. **Probe:** If important, could you explain how registering a device for use on an organisation's network was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

6. Prior to a user's mobile device to being lost or stolen, how important is the need for employee to give access to IT department to enable remote to wipe the data on the mobile device?
  - a. **Probe:** If important, could you explain how enabling remote access to employee mobile device was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

7. Encryption software can be used to encrypt only certain segments of data on a mobile device. How important is the need to implement data encryption shared across information systems in an organisation?

- a. **Probe:** If important, could you explain how implementing data encryption was considered sufficiently in your organisation's BYOD policy?
- b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

8. Using a strong password on a mobile device can be a simple yet effective safeguard. How important is the use of strong password a criterion to accessing an organisation's network?
  - a. **Probe:** If important, could you explain how enforcing the usage of strong password was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

9. A VPN functions on the principle of establishing a channel between the virtual private network servers that is located within the organisation's information system. How important is the need to set-up access controls to verify the identity of a user before granting access to a system on the network?
  - a. **Probe:** If important, could you explain how setting up access controls (firewalls, VPNs) was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

## **EMPLOYEE EDUCATION**

10. How important is the need to educate employees on the purpose for a BYOD policy within an organisation?
  - a. **Probe:** If important, could you explain how educating employees on the need for a policy was considered sufficiently in your organisation's BYOD policy?
  - b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]



11. How important is the need to train employees to raise awareness of threats that are facilitated by user negligence or unawareness within an organisation?
- Probe:** If important, could you explain how train employees to raise awareness of threats that are facilitated by user negligence or unawareness were considered sufficiently in your organisation's BYOD policy?
  - Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

12. How important is the need to encourage and motivate employees to commit to security guidelines and policies within an organisation?
- Probe:** If important, could you explain how encouraging and motivating employees to commit to security guidelines and policies was considered sufficiently in your organisation's BYOD policy?
  - Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

## MOBILE LEARNING

13. Mobile devices could be used for common desktop application utilities, including productivity related microapps. How important is the need for an organisation to allow mobile devices to be used for learning purposes with regards to their roles within an organisation?
- Probe:** If important, could you explain how allowing the use of mobile device to be used for learning purpose was considered sufficiently in your organisation's BYOD policy?
  - Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

14. A wireless mobile device overcomes the limitations of desktop or even laptop computers as they can leverage a wireless carrier's network to access the Internet/Intranet. How important is the need for organisation to allow mobile devices to be used as a communication tool within an organisation?
- Probe:** If important, could you explain how allowing the use of mobile device to be used for communication was considered sufficiently in your organisation's BYOD

policy?

- b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

15. Mobile devices are seen as a way to streamline lengthy business workflow. How important is the need for an organisation to allow microapps to be used as business tools to streamline its workflow?

- a. **Probe:** If important, could you explain how allowing the use of microapps to be used for streamlining business workflow was considered sufficiently in your organisation's BYOD policy?

- b. **Allow for flexibility:** If not important, could you explain why this is not important?

[Researchers comments]

[Reflective notes from the researcher]

Thank you for participating in the interview. At the end of this research, a copy of the research study would be sent to your organisation on request as a sign of appreciation for volunteering to take part in the study.

## Appendix E: Proof of Editing Letter from the Editor

To: Solomon Omokehinde

Email: [solomonomokehinde@gmail.com](mailto:solomonomokehinde@gmail.com)

Contact Number: 0617794253

22 May 2019

Dear Sir/Madam,

This serves to declare that I have read and edited **Mr. Solomon Omokehinde's** thesis for spelling, punctuation, grammar and formatting.

Thank you Kindly,

Rubaphen Yegabaram

CEO, *Magnify Mega Media*

## Appendix F: Gatekeeper Letters

Site 5  
1B Old Main Office Park  
68 Old Main Road  
Kloof, 3613

081 832 4416  
byrd@lfor.co.za  
www.lfor-mobile.co.za



27 July 2016

Mr Solomon Oluwaseun Orokohinfe  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

### RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorisation, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting Interview with Full time Senior IT staff(s) at our premises.

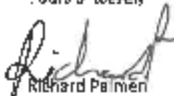
Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely

  
Richard Palmer  
Director





27 July 2016

Mr Solomon Oluwaseun Omokereinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UZM  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with Full-time Senior IT staff(s) at our premises.


Please ensure that the following appears along with your interview documents:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely

  
May-Gene Febbleche  
Director



F (+27) 81 925 7298  
 F (+27) 86 829 9852  
 E [finance@optimumfreight.co.za](mailto:finance@optimumfreight.co.za)  
 W [optimumfreight.co.za](http://optimumfreight.co.za)

P P.O.Box 22449, Cleaaship,  
 Durban, KwaZulu Natal,  
 South Africa, 4022  
 P 21 Aurora Drive, 1st floor,  
 Liberty Park, Lmbalanga Ridge,  
 Durban, KwaZulu Natal,  
 South Africa, 4201

27 July 2016

Mr Solomon Dluwaseun Dmokehinde  
 School of Management, IT & Governance  
 College of Law & Management Studies  
 Westville Campus  
 UKZN  
 Email: 214577345@st.julius.ac.za

Dear Mr Solomon

RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with Full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details,
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely

Steven B.G.  
 Director



Coating & Process Specialist  
t: +27 (0)86 408 3341  
e: markterblanche@primeinspection.co.za  
p: Posinet Suite 537, Private Bag X4, Klood, 3640  
w: www.primeinspection.co.za



27 July 2015

Mr Solomon Doyaseun Omokheinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization wide Bring Your Own Device (BYOD) Strategy for Adaption"*

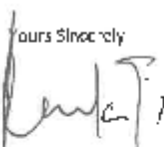
It is noted that you will be constituting your sample by conducting interview with Full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be created with due confidentiality and anonymity

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely  
  
Mark Terblanche  
Director



## Inspired Innovation

**Head Office**  
17 Clark Road, Westmead  
031 701 4988  
info@rigana.co.za

**JHB Office**  
Prosper Business Park, Boksburg  
087 353 9924  
sales@rigana.co.za



27 July 2016

Mr Solomon Oluwaseun Omokehinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
LKZA  
Email: 214577345@stu.jica.ac.za

Dear Mr Solomon

### RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with Full-time Senior IT Staff(s) at our premises.

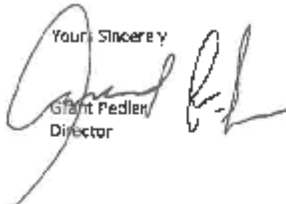
Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated here-within.

Yours Sincerely

  
Grant Pedler  
Director



2 August 2016

Mr Solomon Olujawele Omosaleinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Re: Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organisation towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be conducting your sample by conducting interview with Full-time Senior IT staff(s) of our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them;
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely



Vanessa Talbot

Director

27 July 2016

Mr Solomon Okwaseon-Eromorhinde  
School of Management, IT & Governance  
College of Law, Business & Management Studies  
Wesleyville Campus  
1672H  
Email: 214577346@student.wvu.ac.za



Dear Mr Okwaseon

RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorisation, hereby granting you the needed assistance to conduct research at our institution towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organisation-wide Bring Your Own Device (BYOD) Strategy in Africa"*

It is noted that you will be conducting your sample by conducting interview with Full-time Senior IT Staff in our institution.


Please ensure that the following appears along with your interview documents:

- Letter from your supervisor indicating your research status and dates
- One page summary of the research, as included in the research proposal approved by your supervisor
- Consent form attached to the interview document
- Approval from your supervisor indicating to carry out this research.

Data collected must be treated with due confidentiality and integrity.

You are not authorized to receive letters for any other reasons outside the case stated above.

Yours Sincerely

  
Hans Erasmus JB  
Director

Extreme Innovations  
26 Clark Road, Tlopheng  
T: 031 902 3536  
F: 031 902 3544

PO Box 24532, Brixton Bld, 4110  
E: info@extremee.co.za  
W: www.extremee.co.za  
R: CK 2009/025376/23



Special Leonardo Centre:  
082 451 2744  
www.kyushu@ukzn.ac.za  
www.highwayjka.co.za

Special Catherine McKay:  
085 276 5832  
catherine@highwayjka.co.za  
Highway JKA Karate



27 July 2016

Mr Solomon Dluwaseun Omokehinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our institution towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be consulting your sample by conducting interview with Full-time Senior IT staff(s) at our premises.

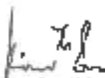
Please ensure that the following appears along with your Interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the Interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herein

Yours Sincerely

  
Kim Sun Wi  
Director



27 July 2016

Mr Solomon Dlwasewu Dinkoehinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated foregoing

Yours Sincerely

  
Fay Kipin  
Director

Head Office: Durban | 570 Inanda Road Unit 9 Newlands West | 4001 | KZN | South Africa

031 765 8648  
0865 0865 49  
Unit 1B (Standard Bank building), 3 Inanda Road, Hillcrest, KZN, 3650  
P.O. Box 688, Hillcrest, 3650  
info@bikini.co.za  
www.bikini.co.za

THE ADVERTISING AND DESIGN GROUP



27 July 2016

Mr Solomon Oluwaseun Omokehinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Western Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting Interview with Full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered Institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the Interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely

Marco Filie  
Director

27 July 2016

Mr Solomon Duvaseur Duvaseur@du  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577345@stu.ukzn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorisation, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with Full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the Interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely



Charlene Erasmus  
Project Manager



21 Gerth Road, Berea, Durban, 4091  
061 779 4253

27 July 2016

Mr Solomon Oluwaseun Onokobin  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UCZN  
Email: 214577345@stu.wcqn.ac.za

Dear Mr Solomon

**RE: PERMISSION TO CONDUCT RESEARCH**

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting interview with Full time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your Interview document:

- Letter from registered institution stating your status with them
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the Interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated herewith.

Yours Sincerely

  
Emilié May  
Project Manager

**TRADING DETAILS: APPRISE.CO.ZA, A DIVISION OF APPRISE (PTY) LTD**





27 July 2016

Mr Solomon Oluwaseun Omokehinde  
School of Management, IT & Governance  
College of Law & Management Studies  
Westville Campus  
UKZN  
Email: 214577545@stu.ukzn.ac.za

Shop No 08, The Place,  
15 Zennith Drive,  
Ilombisa Ridge,  
Durban

t: 031 584 7272  
f: 082 534 8050  
e: sales@aliceroy.co.za  
w: www.aliceroy.co.za

Dear Mr Solomon

RE: PERMISSION TO CONDUCT RESEARCH

This letter serves as an authorization, hereby granting you the needed assistance to conduct research at our organization towards the successful completion of your postgraduate studies. We note the title of your research project is:

*"Factors to consider when developing an organization-wide Bring Your Own Device (BYOD) Strategy for Adoption"*

It is noted that you will be constituting your sample by conducting Interview with Full-time Senior IT staff(s) at our premises.

Please ensure that the following appears along with your interview document:

- Letter from registered institution stating your status with them;
- One Page details of the research, to include the researcher and the supervisor contact details;
- Consent form attached to the interview document;
- Approval from registered institution to carry out this research.

Data collected must be treated with due confidentiality and anonymity.

You are not authorized to use this letter for any other reason aside the one stated hereon.

Yours Sincerely,

Alton Bowen  
Director