COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

- NonCommercial — You may not use the material for commercial purposes.

- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

An Evaluation of Information Technology Risks from the Use of Personal Mobile Devices for Work Purposes

Tshimangadzo Brenda Sikhala

(200704863)

A dissertation submitted in fulfilment of the requirements for the degree of Master’s in Commerce in Computer Auditing at the College of Business and Economics UNIVERSITY OF JOHANNESBURG

Supervisor: Vanessa Van Dyk
Co-Supervisor: Pranisha Rama

2019
Declaration

DECLARATION

I certify that the minor dissertation submitted by me for the degree Master’s of Commerce (Computer Auditing) at the University of Johannesburg is my independent work and has not been submitted by me for a degree at another university.

Tshimangadzo Brenda Sikhala

____________________________
(Name in block letters – no signature)
ACKNOWLEDGEMENTS

I wish to extend my heartfelt gratitude to the following people who contributed to the successful completion of this limited scope dissertation:

- My Little Brother, Vincent Sikhala, Thank you for being a shoulder to cry on when this journey got emotionally draining, dark and lonely. You have been a strength. Thank you for your continued love and support;
- PricewaterHouseCooper my former employer, for their continuous support throughout the journey;
- My Mother, Victoria Sikhala. Thank you for being my pillar and rock throughout this journey.
- All my friend and colleagues who supported me.
- My supervisor and co-supervisor, Vanessa Van Dyk and Pranisha Rama respectively. Thank you for your effort in helping me achieve this milestone. I have learnt so much from you. Your work ethic is incredibly strong and desirable;

Above all, I give all glory and honour to the Almighty God, who afforded me this opportunity, granted me the grace and strength to successfully complete this limited scope dissertation and blessed me with everyone who supported me through it. None of this would be possible without you.
ABSTRACT

Bring Your Own Device (BYOD) is a practice that has gained increasing popularity in recent years. Now, BYOD is being formally acknowledged and techniques have been developed to fully embrace this phenomenon in the workplace. The purpose of this study is to determine the IT risks that arise when employees are allowed to use their personal mobile devices for work purposes to ensure that customer needs are met, and ultimately, to achieve the organisation’s objectives. It is important to analyse how secure the organisation would be if it decided to adopt BYOD. This is achieved by considering the information security policies that organisations have implemented to mitigate the risks inherent in adopting BYOD.

The research question was addressed through qualitative and quantitative methods. Qualitative research was used to obtain secondary data, which involved the investigation of BYOD, its benefits and challenges. Quantitative research was used to evaluate the mobile device policies of the four biggest commercial banks in South Africa through a questionnaire. The questionnaire was based on seven security principles that should be applied according to best practice.

The findings indicated that all of the sampled banks had a common understanding of IT risks that could impact the organisation as a result of BYOD. Effective controls were implemented by the banks to address these risks.

KEY WORDS:
Information Technology (IT), Bring Your Own Device (BYOD), personal mobile device, threats, IT risks, IT controls, mobile device policy.
# TABLE OF CONTENTS

ABSTRACT iii  
TABLE OF CONTENTS iv  
LIST OF FIGURES vii  
LIST OF TABLES viii  
CHAPTER ONE: INTRODUCTION AND STUDY LAYOUT 1  
1.1 INTRODUCTION 1  
1.2 BACKGROUND TO THE STUDY 3  
1.3 RESEARCH STATEMENT, QUESTIONS, OBJECTIVES AND SIGNIFICANCE OF THE STUDY 5  
1.3.1 Research statement 5  
1.3.2 Research question 6  
1.3.3 Research objectives 6  
1.4 RESEARCH METHODOLOGY 7  
1.5 OUTLINE OF THE CHAPTERS 8  
1.6 CONCLUSION 9  
CHAPTER TWO: LITERATURE REVIEW 10  
2.1 INTRODUCTION 10  
2.2 DEFINITION OF BYOD 12  
2.3 CHARACTERISTICS OF BYOD 13  
2.4 BENEFITS OF BYOD 14  
2.5 CHALLENGES OF BYOD 15  
2.5.1 Mobile device threats and related risks 17  
2.5.1.1 Malware 17  
2.5.1.2 Loss or theft of devices 20  
2.5.1.3 Malicious insider actions 20  
2.5.2 Key risks stemming from BYOD threats 21  
2.6 SECURING A BYOD ENVIRONMENT 22  
2.7 RISK ASSESSMENT PRIOR TO IMPLEMENTING BYOD 23  
2.8 MITIGATION OF BYOD IT RISK 25  
2.8.1 Mobile device policy 27  
2.9 CRITICAL LINKS TO THE EMPIRICAL RESEARCH 36  
2.10 CONCLUSION 37  
CHAPTER THREE: RESEARCH METHODOLOGY AND DESIGN 39
3.1 INTRODUCTION

3.2 RESEARCH DESIGN

3.3 RESEARCH METHODOLOGY

3.3.1 Research approach

3.4 POPULATION AND SAMPLE

3.5 RESEARCH INSTRUMENT

3.6 DATA ANALYSIS AND INTERPRETATION

3.7 VALIDITY AND RELIABILITY

3.8 ETHICAL CONSIDERATIONS

3.9 CONCLUSION

CHAPTER FOUR: RESEARCH FINDINGS AND ANALYSIS

4.1 INTRODUCTION

4.2 QUESTIONNAIRE RESPONSE RATE

4.3 RESEARCH PARTICIPANTS

4.4 RESEARCH FINDINGS

4.4.1 Do you have a mobile device policy in place? And do you believe the policy has added benefit in how the organisation manages risk?

4.4.2 How often is the policy updated?

4.4.3 Are employees’ personal mobile devices on-boarded onto the organisation’s network?

4.4.4 Do you offer any training to employees prior to on-boarding their device and if yes, what kind of training do you offer?

4.4.5 What are the major IT risks that your organisation is exposed to when employees use their personal devices for work purposes?

4.4.6 Do you allow employees to download external applications that are not approved by the organisation onto their personal devices?

4.4.7 Have you had any incidents of data breach as a result of employees using personal devices for work?

4.4.8 Describe some of the controls that the organisation implements to mitigate the risks that emanate from BYOD and how do you control these risks?

4.4.9 Do you believe that the IT controls that your organisation has implemented are effective to mitigate the risks the bank is concerned about?

4.4.10 Do you have controls in place to ensure that the privacy of employees’ personal information contained on the mobile device is maintained?

4.4.11 Are the bank’s infrastructure, mobile device operating systems and applications regularly updated to resolve security vulnerabilities and threats?

4.5 CONCLUSION

CHAPTER FIVE: CONCLUSION
LIST OF FIGURES

Figure 1: Distribution of new mobile malware by type 18
Figure 2: New mobile malware discovered 18
Figure 3: MDM architecture 26
Figure 4: BYOD policy architecture 28
Figure 5: Overview of mobile device policy usage across the sample banks 49
Figure 6: Analysis of how often banks update their mobile device policy 50
Figure 7: Analysis of whether employees are on-boarded onto the organisation's network 51
Figure 8: Analysis of training and awareness that employees are offered 52
Figure 9: Analysis of incidents the banks suffered because of BYOD 55
Figure 10: Analysis to determine whether controls implemented are effective 57
Figure 11: Analysis of whether employees' privacy is maintained 58
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Keys risks related to BYOD operations</td>
<td>21</td>
</tr>
<tr>
<td>Table 2</td>
<td>BYOD environment architectural principles</td>
<td>29</td>
</tr>
<tr>
<td>Table 3</td>
<td>Sample selected</td>
<td>42</td>
</tr>
<tr>
<td>Table 4</td>
<td>Response rate</td>
<td>48</td>
</tr>
<tr>
<td>Table 5</td>
<td>Research participants</td>
<td>49</td>
</tr>
<tr>
<td>Table 6</td>
<td>Analysis of some of the controls the banks have implemented</td>
<td>56</td>
</tr>
</tbody>
</table>
CHAPTER ONE: INTRODUCTION AND STUDY LAYOUT

1.1 INTRODUCTION

In the early 1990s, Information Technology (hereafter IT) became the main driver of most businesses as organisations increasingly turned to IT to enhance productivity and reduce operating costs. A study conducted by the Society of Information Management in 2010 indicated that business productivity and cost reduction was a key priority for global organisations, ranking fourth on the list of top management concerns (Arregui, 2015:3).

Successful businesses today thrive on global presence and a workforce that appears to be everywhere at once by using the internet. The internet economy is no longer a niche marketplace, but rather a business delivery mechanism which has become embedded in every organisation. A number of emergent technologies also identified mobile and wireless technologies as the fastest growing area of technology investment globally (Dedeche, Liu, Le & Lajami, 2013:2).

Information technology has also fundamentally reshaped the banking industry as banks use technology to support and enhance their relationships with customers through the cross-selling of customised products and innovative services. Whether the intention is to broadcast their business services, transact electronically or generate new customers and market segments, almost every organisation, large or small, faces the challenge of managing a reliable, secure and competitive presence through technology (Calder, 2011:8).

It has been noted that organisations are slower to adapt to change than individuals when it comes to new technology as they tend to focus more on protecting their resources. When such resources are not protected adequately, this can result in financial losses and may have a negative impact on the functioning and future operational effectiveness of the business. Information security is a concept that was designed specifically to help organisations to protect information assets. The right information security controls need to be implemented to address IT risk within an organisation. These controls can be implemented through effective IT governance, processes, strategy and policies designed to address issues that evolving IT poses (Tallon, 2013:1). This allows organisations to
function effectively in meeting their objectives and goals, ensuring that employees are productive at all times, while reducing operational costs (Ulrich & Smallwood, 2004:5).

To ensure that employees are more productive, they need to have the flexibility and convenience of working anywhere, at any time. Many organisations then have little option but to allow employees to use their own personal devices for work-related activities (Ghosh, Gajar & Rai, 2013:2). This allows employees to access the organisation’s resources, respond to client emails anywhere at any time, simply by connecting to the organisation’s network using their personal device (Arregui, 2015:1). This phenomenon is referred to as Bring Your Own Device (hereafter BYOD).

According to Bais (2016:9), BYOD collectively refers to:

...the related technologies, concepts, policies, and strategies where the employees can access corporate data of the company and internal IT infrastructure such as database and applications, using their personal mobile devices such as smart phones, the laptop computers and the tablets PVs.

The trend of BYOD has been rapidly adopted by many organisations despite the disadvantages of deployment (Bello, 2015:6).

A study conducted by Alleau and Desemery (2013:6) indicates that employees who use mobile devices for both work and personal use end up working an additional 240 hours per year compared to those who do not. The study also indicated that BYOD creates an environment where employees are motivated to work as they are able to work even when they are at home using their personal devices. Wang, Wei and Vangury (2014:40) reveal that when employers allow their employees to use their own personal devices for work, they create the flexibility of working from anywhere at any time.

There are a number of benefits associated with BYOD that have been identified and this will be discussed in detail in Chapter Two. However, although BYOD has numerous benefits, it also introduces many risks to the organisation. These include the loss of devices or weak credentials, which may undermine the confidentiality of client information contained on the device. Other risks include data leaks and malware attacks, which may compromise data consistency and potentially cause complete data loss (Bello, 2015:6). It is important for BYOD to be implemented appropriately, taking into account current and emerging IT risks. The successful implementation of the BYOD initiative also demands
that organisations modify their policies, train their employees and tighten information and communication technologies security (De Haes & Van Grembergen, 2015:9).

Two major risks highlighted in this study include (i) the lack of security protection, which has an impact on the confidentiality, integrity and availability of the organisation’s resources, and (ii) the violation of employee privacy with regard to employees’ personal information contained on the mobile device. When personal devices are used for work purposes, it is usually assumed that the risk of employee negligence on the device will be transferred to the organisation (Chia, 2012:1).

It is important for the organisation to perform risk assessment procedures before an employee is allowed to use their personal mobile device for work purposes. This will provide the organisation with a holistic view of the security threats and privacy issues stemming from BYOD. With the myriad IT risks that an organisation has to consider, it is also important to clearly define the responsibility of securing the organisation’s data. This can be resolved by implementing proper IT security policies related to BYOD (Garba, Armarego & Murray, 2015:191).

1.2 BACKGROUND TO THE STUDY

Over the last decade, it has become common practice for employees to have dual-use computing devices, which are used for both private and work purposes, and often for a mixture of private and work purposes. A recent survey indicated that 95% of companies allow employees some use of their own devices, 36% offer full support of all employee-owned mobile devices while 48% support selected devices (Chen & Zhao, 2012:4).

BYOD is a concept that has evolved over time and gained increasing momentum in the workplace (Schalow, 2013:10). Most employees bring their personal mobile devices to work and later continue their work at home from their personal mobile devices (Sayah, 2013:179). This is all possible when an organisation allows employees to connect to its network through their personal device.

According to Bais (2016:4), this concept was introduced to South Africa in 2009 as new smartphones emerged and employees carried their smartphone everywhere they went. With the influx of new devices in early 2010, employees started bringing their personal
devices to work regardless of whether IT departments supported them or not. Most Chief
Information Officers (hereafter CIOs) began experiencing security pressures as a result
of accommodating these devices and responded by blocking all personal devices from
the organisation’s network (Kamau, 2013:3).

In late 2010, a number of Mobile Device Management (hereafter MDM) programmes were
released to provide the first Application Programme Interface (API) to allow organisations
to manage personal devices better. Most organisations and IT departments understand
that they cannot disregard BYOD any longer (Mathur, Agarwal & Sharma, 2015:6). In
2012, most IT departments started facing security challenges that came with BYOD due
to data leakages and employees becoming concerned about their privacy on their

Organisations started focusing on policies and frameworks to address employees’ privacy
concerns while at the same time addressing any IT risks stemming from personal mobile
devices connected to the organisation’s network. MDM became a solution for most
organisations (Mitrovic, Thompson, Vekjkovic & Whyte, 2014: 18). MDM is a software tool
that is used to manage a device security controls such as locking down the device, remote
wiping and data backup on the device.

In 2013, applications and security were the main focus of BYOD and organisations were
searching for additional security measures to manage their resources (Bais, 2016:13). Organisations then began to expand their management platform from MDM to Mobile
Application Management (MAM) (Morrow, 2012: 3). MAM is similar to MDM but the
difference is that it is used to manage specific security control applications in the device.

BYOD goes beyond just employees having access to their emails; they have full access
to the organisation’s network and are able to access their organisation’s resources at any
time (Bais, 2016:13 & Webroot, 2013:4). In 2015, organisations began to focus more on
the security impact that BYOD brought with it and developed additional mechanisms to
minimise potential risks faced by an organisation (Mitrovic, et al., 2014:7). Although the
BYOD is not a new trend, This has created a new shift in how banks and other financial
institutions approach consumerisation of IT. The Chief Information Officers (CIOs) and
other bank executives remain wary of security issues when employees use their personal
devices for work purposes they are also embracing consumer IT within the enterprise as
an opportunity to drive efficiency and innovation, as well as to increase both employee and customer satisfaction. The risks of information risk increase as the bank is not only worried about about the technology controls, they must consider people risks as an element of leaking or exposing confidential information using their personal devices (Informationweek, 2012:1).

This study focuses on IT risks that arise when employers allow their staff to use their personal devices for work purposes as part of business operations. The study also seeks to determine whether organisational resources are secured and whether employee privacy on their device is protected.

**1.3 RESEARCH STATEMENT, QUESTIONS, OBJECTIVES AND SIGNIFICANCE OF THE STUDY**

**1.3.1 Research statement**

Although there is evidence that BYOD brings benefits for both the employee and the employer, there are also a number of risks that should be considered and maintained at an acceptable level before the employer allows personal devices to be used for work purposes. For instance, if sensitive data is stored on poorly secured mobile devices and the device is stolen or lost, an attacker may be able to gain access to confidential data and impact the organisation’s reputation if exposed to the public (Niharika, 2012:4).

Financial intermediaries play a pivotal role in the performance and operation of modern economic activities. Banks remain one of the key financial intermediaries in an economy, providing a variety of services. The efficiency of financial intermediaries can have a significant impact on modern economies. A stable and profitable banking sector is able to resist negative shocks and contributes to the stability of a country’s financial system (Dietrich & Wanzenried, 2009:1).

Although there are many risks within the banking environment, namely, solvency, liquidity, credit or price risk, the most critical risk that may have an impact on a bank is IT risk. Valid information is an important factor that leads to the success of the business. Therefore, information systems and IT infrastructure are considered as the most strategic capital for any business. Personal devices operate outside the protection of the banks’ IT
infrastructure which makes the organisation’s information particularly vulnerable to security breaches (Teymouri & Ashoori, 2011:1).

The confidentiality, integrity and availability of the organisation’s information must be supported by the mobile device to ensure that the organisation continues to operate both effectively and securely at all times (Miller, 2016:25). Therefore, it is important to evaluate IT risks that arise from using personal mobile devices for work purposes. The research statement can therefore be formulated as follows:

- An evaluation of information technology risks arising from the use of personal mobile devices for work purposes.

1.3.2 Research question

The purpose of this study is to evaluate IT risks that arise from allowing employees to bring their personal mobile devices to work, connect them to the organisation’s network and use these devices for work purposes as part of their daily operations. On the one hand, this ensures that employees are productive at all times while the organisation is meeting its business objectives. On the other hand, however, it is also important to evaluate the negative effects that this may have on the organisation.

The following research question will therefore be used to determine the safety of using personal mobile devices for work purpose:

- What IT risks are associated with the use of personal mobile devices for work purposes?

1.3.3 Research objectives

The evidence that was gathered in this study made it possible to address the research question stated in section 1.3.2 above and to meet the following research objectives:

- Identify risks that are likely to exist when an organisation allows its employees to use their personal devices for work purposes.
- Evaluate controls that identify, assess and manage the information technology threats associated with the use of personal mobile devices for work purposes.
- Identify whether the information security policies of the Big 4 banks are addressing IT risks arising from the use of personal devices for work purposes.
1.3.4 Significance of the research

This study identifies IT risks that commonly emerge when allowing personal devices to be used for work purposes and highlight frameworks and controls that can assist organisations to minimise these IT risks.

IT risk within the banking industry is paramount, particularly in view of the ongoing financial and economic crises as a result of cyber-attacks, when allowing employees to use their personal devices for work. Information technology risk impacts the banking industry in most countries around the world and it is important to evaluate IT risk and identify the minimum controls that should be in place (Dietrich & Wanzenried, 2009:1).

1.4 RESEARCH METHODOLOGY

A literature review is conducted in Chapter Two on IT risks associated with the use of personal mobile device for work purposes. This review seeks to obtain an understanding of why employers and employees allow personal mobile devices to be used for work purposes. It also considers the current IT risks that come along with adopting BYOD. Information security frameworks and standards are also examined to assist in addressing any risk as a result of BYOD.

The empirical component of this study is conducted by selecting a sample of South African banks. The sample is based on the four largest banks in the country which represent 85% of the banking market share. According to Business Technology (2018:1) and the Banking Association of South Africa (2018:1), Standard Bank, FirstRand, Absa (Barclays Africa) and Nedbank were the four biggest commercial banks in 2018 based on asset value. Information security policies implemented within these banks are evaluated to determine whether the minimum IT security criteria have been addressed in their policies. Section 1.5 below describes the approach adopted to answer the research question and meet the research objectives.

The research methodology that is followed in this study consists of an analysis of secondary data in the field of BYOD, and more specifically, IT risks that both employers and employees are likely to encounter when personal mobile devices are used for work purposes. Qualitative research seeks to elaborate, explain or analyse management
theories; it uncovers experiences, processes and causal mechanisms through its unconventional methods (Dedeche et al., 2013:1870). In answering the research question and ensuring that the research objectives are met, non-numerical and minimum numerical data will be used to evaluate IT risks stemming from the use of mobile devices for work purposes.

1.5 OUTLINE OF THE CHAPTERS

This study consists of five chapters, summarised as follows:

Chapter 1: Introduction
This chapter introduces the background to the study and the research problem, which is the safety of the organisation’s resources when employees use their personal devices to access the organisation’s network in carrying out their daily tasks to meet organisational objectives, and ultimately, the needs of customers. The research problem is further broken down into one research question and three research objectives. This chapter also covers the research methodology and approach.

Chapter 2: Literature review
This chapter focuses on existing literature on BYOD and the associated IT risks. The following is covered:
- Definition of BYOD
- Characteristics of BYOD
- Benefits of BYOD
- Challenges of BYOD
- Responsibilities for securing BYOD
- Risk assessment prior to implementing BYOD and mitigation of BYOD IT risks.

Chapter 3: Research design and methodology
This chapter outlines the research methodology used in this study. It consists of the research design and details the steps of the research process to evaluate mobile device policies of the four biggest banks in South Africa.

Chapter 4: Empirical study and research findings
This chapter describes the extent of IT risk and controls provided in the four biggest banks’ policies as they relate to mobile devices. Data is obtained through a questionnaire.

**Chapter 5: Conclusion**

This chapter presents a summary of the literature review conducted in Chapter Two and the empirical research of Chapter Four. Areas for future research are suggested and a consolidated view of whether the research objectives were achieved is provided.

1.6 CONCLUSION

This chapter lays the foundation of the study by providing the background and describing the IT risks associated with allowing personal mobile devices to be used for work. This chapter further outlines the problem statement, research objectives, research methodology and the research approach. The importance of investigating and addressing IT risks is justified.

The benefits of BYOD are discussed briefly, in particular, the benefits of allowing employees to use their personal devices for work purposes. It is also important to highlight IT risks associated with BYOD from both an employer and employee perspective. The next chapter presents the literature review.
CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

The development of technology has fundamentally changed the way organisations do business. Today, most organisations’ digital operations and even their existence is inconceivable without the extensive use of IT. Due to the accelerating shift away from desktop to mobile device usage, the consumerisation of BYOD has become the subject of considerable interest in the IT industry and digital operations within corporates. IT provides the foundation for new products, services and ways of conducting business; it provides organisations with a strategic advantage as it makes ways of working easier and more productive (Safari & Khalaf, 2013:1).

The development of IT has reshaped the banking industry and has set the foundation for new products and services. These create a strategic advantage to meet the customers' needs at all times. This study evaluates IT risks within the banking industry resulting from employees’ use of their personal devices for work purposes (Love, Irani & Edwards, 2004: 509). Banks can also export economies of scale and scope that are derived from standardised IT support processes, which are mainly presented in transaction banking (Marinč, 2013:72).

IT has also enhanced the ability of banks to process and transmit quantifiable data and has created an environment where banks have to decide whether to do transactional banking or relationship banking. IT-driven marketability and structural changes may reinforce each other and culminate in increased systemic risk. Risk-taking by individual banks may become highly correlated with each other and this may increase the probability that banks fail simultaneously (Marinč, 2013:1; Bessis, 2011:6).

The same can be said of other organisations globally which are continuously looking for new ways of increasing employee productivity, efficiency and flexibility through IT (Shah, 2015:47). Mobility has now become a topic of discussion in many organisations which are looking at incorporating mobile initiatives into their day-to-day operations. The challenge arises when IT executives struggle to accommodate the number of devices used for work purposes in their IT infrastructure, mainly because employees are not only demanding
access to the organisation’s network but are also demanding access to networks beyond the organisation’s firewalls via their personal devices (smartphones, home PCs, tablets and home laptops) (Kossek, Lewis, Hammer, Kelliher & Anderson, 2010:62).

There is one important concept that IT executives need to keep in mind, and that is to always protect the organisation’s resources. IT departments should always strive to find new ways to enable, manage and secure the user’s access to the organisation’s resources (Brodin, Rose & Åhlfeldt, 2015:5). Nonetheless, the benefits of BYOD are undisputable and persuasive. Organisations that have adopted BYOD have reported greater employee productivity and retention and increased mobility while employees have greater work flexibility (Bernhard, Bixler, Choudhury, McBurney & Purta, 2013:2).

BYOD has created an environment where employees have the freedom to work anywhere they chose to. However, with all the benefits such as cost reduction, production enhancement and flexibility of working anywhere and at any time, BYOD can also introduce security risks into the organisation if proper controls are not in place (Wang et al., 2014:80). The purpose of this study is to evaluate the IT risks stemming from the use of personal mobile devices for work purposes to ensure that the customer’s needs are met and ultimately, to achieve the organisation’s objectives. It is important to assess how secure an organisation would be if it decided to adopt BYOD.

Mitigating controls such as a BYOD policy is discussed below in section 2.8. Key controls and objectives that should be in place in the policy are also discussed. A policy on key controls and objectives will assist any organisation to manage and mitigate IT risks that arise. Indeed, such a policy is useful as a solution for IT risk irrespective of whether the organisation allows BYOD or not. This section assists in answering the research question listed in section 1.3.2. The following topics are included as part of the literature review:

- Definition of BYOD
- Characteristics of BYOD
- Benefits of BYOD
- Challenges of BYOD
- Responsibilities in securing BYOD
- Risk assessment prior to implementing BYOD
- Mitigation of BYOD IT risks.
In section 2.2 which follows, the concept of BYOD is explored in detail. Various definitions BYOD are considered and documented.

2.2 DEFINITION OF BYOD

Bring Your Own Device (BYOD) can be defined as “An IT policy where employees are allowed or encouraged to use their personal mobile devices such as iPads, smartphone, etc. to access the organisation’s data and systems” (IBM, 2017:1). BYOD can further be defined as the use of personal devices for work and personal purposes and it reflects a blurred line between personal and business use on the same device (Wang et al., 2014:80).

Ketel and Shumate (2015:1) see BYOD as a corporate trend where employees are allowed to bring their personal devices to work and use them for both personal and work purposes. Deloitte (2016:3) define BYOD as the use of employees’ personal devices to access the organisation’s content or network. Bais (2016:9) offers a broader view of BYOD, which he collectively refers to as:

…the related technologies, concepts, policies, and strategies where the employees can access corporate data of the company and internal IT resources such as databases and applications, using their personal mobile devices such as smartphones, laptop computers and tablets.

From all the above definitions, BYOD is seen as an IT trend and a broader movement that impacts the way an organisation conducts business, invests in its assets, empowers employees and increases the ability to attract and retain talent (Bello, Armarego & Murray, 2015:1279).

However, BYOD as defined by the press or the media, is often confused. Definitions are broad, mainly because BYOD enables and impacts other trends such as devices, the consumerisation of information technology, cloud computing as well as virtualisation. Bello (2015:13) and Ketel and Shumate (2015:1) clarify that BYOD can be seen as an environment where employees use personal technology such as smartphones, home PCs and laptops to access the organisation’s network, applications and data.
BYOD is now considered to be the most popular model for an organisation because it provides flexibility for employees. This is in line with current trends as today’s business environment is demanding more flexible hours from employees. With the expanding ecosystem, employees are requesting to access the organisation’s applications, networks and data from anywhere and at any time using their personal devices through a BYOD programme (McQuire, 2012:1 & Bernhard et al., 2013:2).

From the above definitions, the term BYOD can collectively be referred to as technologies, concepts, strategies and policies where an employee is able to gain access to an organisation’s network and internal resources using their personal device such as a laptop, smartphone or iPad for work purposes. The application of BYOD is spreading because of the mutual benefits that are derived between the organisation and the employees (Zulkefli, Singh & Malim, 2015:2).

There are several characteristics of BYOD which are discussed in detail in the next section.

2.3 CHARACTERISTICS OF BYOD

As mentioned in the previous section, BYOD enables employees to use their personal devices for work purposes. This new technology also allows employees to work from any environment. From the definition above, it was noted that mobility, mobile environment, mobile technology, mobile computing and consumerisation are all key characteristics of BYOD. This section discusses these characteristics in detail.

- **Mobility:** Mobility is defined as a situation of not being limited to a geographic location yet being able to access information anywhere at any time (Mitrovice, Veljkovic, Whyte & Thompson, 2014:5). BYOD is defined as a process where the employer allows employees to use their personal device for work purposes, hence BYOD is characterised by mobility as employees are able to work from anywhere at any time using their personal device (Shah, 2015:47). Mobility does not restrict employees from working at one workstation or an office desktop.

- **Mobile Environment:** A mobile environment is one where people are in motion and have access to the applications, files and services they require to do their job wherever they are. In this environment, employees are more likely to be productive
as they are using their personal devices for work purposes (Scarfo, 2012:446). Studies show that BYOD increases productivity as employees are not limited to working the normal eight hours at the office. Employees are able to respond to work emails and attend to other work-related duties while on a bus on their way home or at home (Ghosh et al., 2013:63).

- **Mobile Technology**: Mobile technology refers to a technology that can easily be carried around and can be used by individuals on the move. With BYOD, employees’ devices such as smartphones and iPads can be easily carried around; they are portable as they are designed to be used by moving individuals. They provide employees with the flexibility of working while they are in motion (Mitrovic et al., 2014:4).

- **Mobile Computing**: Mobile computing in BYOD is defined as “Technology that enables individuals to access the network services anywhere and anytime” (Kamau, 2013:10). BYOD enables employees to access the organisation’s network at anytime and anywhere using either Virtual Private Network or their own mobile data.

- **Consumerisation**: Niehaves, Köffer and Ortbach (2012:1) define consumerisation as the choice of employees as to the type of device they would like to use, what applications they would like to install on the device and what activities they would like to perform. BYOD creates significant change in the organisation as employees are able to access the organisation’s applications and data anywhere using any device of their choice.

BYOD presents many benefits to the organisation. These benefits provide a view on how BYOD contributes to the organisation’s goals and mission and why most organisations are adopting the BYOD programme as part of their business operations. These benefits are discussed in the next section.

### 2.4 BENEFITS OF BYOD

It is assumed that the BYOD trend has arisen as a result of mobile transition, creating a new generation of employees (Furnell, 2007:1). This suggests that most employees are willing to accept lower pay if organisations are willing to allow flexibility in the work environment. Shah (2015:47) believes that BYOD enhances creativity and innovation and
improves the balance between employees’ professional and personal lives. Additional key benefits of BYOD are covered below:

- **Accessibility:** BYOD allows employees to access the organisation’s network and resources wherever they are and at their own pace. Information is shared faster and is available to employees 24 hours because the network is constantly available (Bello, 2015:16).

- **Employee Satisfaction:** BYOD leads to greater employee satisfaction because they have the freedom to select the device of their choice as opposed to using the devices chosen by the organisation (Bello, 2015:16). By using their own personal device, employees do not have to carry multiple devices with them wherever they go. BYOD enables employees to better balance their personal and professional lives because they can manage both simultaneously (Nah, Siau & Sheng, 2005:88).

- **Increase Productivity and Innovation:** The primary benefit of BYOD from an employer’s perspective is to increase productivity in terms of output as well as collaboration with others. According to Chowdhury and Ghosal (2015:3) and Kamau (2013:10), about 50% of the IT managers claim that when employees are satisfied, productivity is enhanced. When employees are more satisfied and more comfortable working on their own devices, they quickly become experts, hence they become more productive (Shah, 2015:47).

- **Lower costs:** BYOD reduces mobility costs because employees are paying for the costs of their mobile device. Moreover, employees are allowed to work remotely, which reduces the cost of travelling to the office, office space is freed up as most employees are able to work from home, and there is also a greater reduction in labour, printed material and stationery (Singh, 2012:4).

Although there are many benefits that can be derived from BYOD, there are also several challenges which the organisation may encounter. These challenges are discussed in the section below.

**2.5 CHALLENGES OF BYOD**

With all the benefits that BYOD programme introduces, there are also challenges that arise and these should be taken into consideration as part of risk assessment prior to implementing BYOD. Data security is regarded as the most challenging and academic
literature on BYOD accords the greatest attention to this area. Security should be considered regarding every aspect of the organisation’s network, data and applications. The organisation should ensure that its resources and data are separated from personal data (PricewaterhouseCoopers, 2013:4). The fundamental values of confidentiality, integrity, authenticity of the organisation’s data are particularly at risk with BYOD in place (von Solms & von Solms, 2008:9) and most organisations strive to preserve these values.

Confidentiality can be compromised when unauthorised individuals gain access to sensitive information (Wang et al., 2014:81). This can occur by manipulating the device or intercepting data transmission (Wang et al., 2014:81). The integrity of information can be compromised when the device is infected with malware resulting in data being lost or leaked to unauthorised individuals (Mathur et al., 2015:492). The availability of information and application could be impacted when there is an increase in network traffic (Carroll, van der Merwe & Kotze, 2011: 23).

Mobile devices that are insufficiently secured can lead to unauthorised use and modification of data due to deliberate or negligent actions. When employees use their personal devices, it is assumed that they are negligent or that the reckless behavior of users during their private use will be transferred to the organisation. Certain personal devices used by employees are not sophisticated and lack security controls such as anti-viruses, patches, firmware updates and configuration settings which make them vulnerable to threats (Bernhard et al., 2013:2).

Any unauthorised or non-work-related applications on the user’s device have the potential to affect the integrity of the organisation’s data. Moreover, mobile devices use a variety of operating systems. As there are constant changes with technological advancements, these become outdated very quickly. The device can easily be jail-broken when proper controls are lacking. The privacy of employees’ personal data on the device is also regarded as one of the key challenges employees encounter (Vignesh & Asha, 2015:5212).

Because business and personal data co-exist on the same device, it makes it difficult for the organisation to find a balance between strict security controls of the organisation’s data and personal data, specifically when the device is not a corporate-issued asset. In
this study, BYOD challenges are elaborated by discussing three major threats that mobile devices are vulnerable to as well as the associated risks to the organisation.

2.5.1 Mobile device threats and related risks

The challenges enumerated above may introduce malware from the user’s untrusted personal device to the organisation’s network. IT processes and systems can be impacted and in extreme cases, the malware can delete, steal or hold ransom valuable information pertaining to the organisation or its customers.

2.5.1.1 Malware

Anyone who uses technology for either work or recreational purposes is bound to come across one or all of the following threats directly or indirectly: viruses, Trojan horses, botnets, rootkits and worms. All of these threats can be classified as malware. Malware is a well-known threat to BYOD and can pose a threat when organisations do not have proper security controls in place.

The main purpose of malware is to break into the device, spy or steal the user's information and cause damage to the device (Ghosh et al., 2013:63). Attackers often deceive users by requesting them to install malicious software applications on their devices (Ketel & Shumate, 2015:2). In most instances, the hacker waits for an opportunity when the device is vulnerable to access it remotely.

Malware threats are a global issue, affecting most countries that have a significant smartphone base. This can be clearly seen in a study conducted by Securelist (2017:1). As shown in Figure 1 below, in 2017, infection rates of malware increased from the first to the fourth quarter.
These statistics indicate that malware is affecting a large number of mobile devices, looking at the statistics in the McAfee threats report, in 2016 at least 2 000 000 new mobile malware were discovered and in 2017, in just two quarters, about 1 600 000 new mobile malware were discovered. These numbers do not show any sign of abating, which is becoming a growing concern.

**Figure 1: Distribution of new mobile malware by type**

*Source: Securelist (2017:1)*

**Figure 2: New mobile malware discovered**

*Source: McAfee Labs (2017:60)*
In another report compiled by Kaspersky Lab, mobile security products detected about 32 000 mobile banking Trojans. It was also noted that the most common mobile security threats come from viruses, spyware and other malicious programmes. Considering the above statistics, it is clear that malware is an issue that is not going away and should be dealt with (Kaspersky, 2017:1).

Different types of malware are described below:

- **Virus**: A virus is defined as a programme that can infect other programmes by changing them to include a possible evolved copy of the programme. It can spread when the host programme that it is attached to is copied from one device to another through a network, either via file sharing or removable media.

- **Trojan horse**: Hackers gain control over the device by deploying malicious applications to the device. These applications may appear useful to the user, while running malicious activities in the background (Edwards, Jamaluddin & Zotou, 2004:200).

- **Botnet**: A set of devices controlled remotely are referred to as botnets. This method uses computing power to compromise the device to commit various activities such as sending spam mail or Denial of Service (hereafter DoS) attacks (Esahi, Naseri, Hashim, Tahir & Saad, 2014:190).

- **Worm**: A worm is defined as “a self-replicating malicious application designed to spread separately to applications that are not infected” (Edwards et al., 2004:200).

- **Rootkit**: A rootkit is an application that obtains the right to run in a privileged mode. This type of malware modifies the device’s standard operating system functionalities (Baliga, Bickford, Ganapathy, Lftode & O’Hare, 2012:49).

- **Phishing**: This is a method applied by hackers as a means of collecting or forcing the mobile device user to send confidential information to them. This can be used as a mechanism to trick the user into downloading malware onto their device (Leavitt, 2011:13). Other phishing methods include the hacker sending an email to the user, pretending to be a legitimate user and requesting them to reply to a fraudulent email with confidential information (Ghosh, et al., 2013:63). Other mechanisms used by hackers include inviting the user to register their personal details on a website, deceiving users to install software to be able to download files onto their devices (Flores, Qazi & Jhumka, 2016:1009).

- **Direct attacks**: Here, hackers use their intellectual skills to identify and analyse a device and launch an attack against it. The intention of direct attack is to steal, destroy or change confidential information that might have a direct impact on the
organisation’s business operations. A well-known direct attack is known as “Anonymous” and has directly attacked several organisations all over the world (Bello et al., 2015:1280).

- **Data communication interception/spoofing**: One of other major threats to BYOD is data communication interception. This becomes a serious concern when a user sends information over the internet without proper security controls on the network (Bello, 2015:25). Another security concern is when a user is deceived into sending information to the wrong recipient and receives malicious information from an unknown sender through a wireless network (Hansen, 2011:2).

### 2.5.1.2 Loss or theft of devices

Smart devices are an increasing concern to the organisation as they are more likely to be lost as compared to traditional computers, when used for work purposes (Ketel & Shumate, 2015:2). A stolen device may contain valuable and confidential information, which becomes easily accessible to unauthorised individuals who might use this information for fraudulent or illegal purposes (Ghosh et al., 2013:63). With a BYOD programme implemented by most organisations, it is noted that the device becomes less valuable whereas the information contained on the device becomes more valuable (Tu & Yuan, 2012:13).

### 2.5.1.3 Malicious insider actions

These types of attacks have received substantial attention and are considered as one of the most dangerous security issues that an organisation encounters. Many government officials and other organisations have reported how malicious insiders have exposed the company’s confidential information (Richardson, 2008:4).

Hunker and Probst (2011:18) describe malicious attacks as being one of the most difficult security threats to manage. Malicious insiders have direct access to the organisation’s resources and networks, which makes it easy for hackers to steal, destroy or even modify data because they can access the organisation’s resources anytime and anywhere. Phishing, data interception and spoofing can be executed by employees wishing to cause harm (malicious insiders) without the organisation ever realising it (Sarkar, 2010:130).
It can thus be concluded that the key threats that any organisation is likely to encounter when it has adopted BYOD are malware attacks, loss of mobile devices and malicious insider actions. There are specific risks that the organisation may suffer as a result of the threats discussed above. These risks are evaluated in the section below.

2.5.2 Key risks stemming from BYOD threats

There are key risks that organisations adopting BYOD need to consider. Five of these key risks are explained in the table below.

**Table 1: Keys risks related to BYOD operations**

<table>
<thead>
<tr>
<th>Key Risks</th>
<th>Overview of key risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational risk</strong></td>
<td>● Lack of mobile ready support and operational processes.</td>
</tr>
<tr>
<td></td>
<td>● Lack of resources, skill sets and technical capabilities in-house.</td>
</tr>
<tr>
<td></td>
<td>● Highly diverse mobile ecosystem due to multiple mobile operation systems (hereafter OSs) and carrier-specific implementation.</td>
</tr>
<tr>
<td><strong>Legal and regulatory risk</strong></td>
<td>● Potential loss of privacy due to personal activity, device use, data exposure, etc.</td>
</tr>
<tr>
<td></td>
<td>● Ethical and legal issues around monitoring, device wiping, security devices and availability of the organisation’s data on the device upon employee termination, etc.</td>
</tr>
<tr>
<td></td>
<td>● Regulatory requirements regarding e-discovery, monitoring and data archiving.</td>
</tr>
<tr>
<td><strong>Technology and data protection risk</strong></td>
<td>● Lack of native encryption on device, memory cards and at OS level (for certain OSs).</td>
</tr>
<tr>
<td></td>
<td>● Unauthorised and unapproved installation of applications by end users.</td>
</tr>
<tr>
<td></td>
<td>● Interaction with other systems (cloud storage, personal computer synchronisation, etc.).</td>
</tr>
<tr>
<td></td>
<td>● Lack of mobile OS patching and update enforcement.</td>
</tr>
<tr>
<td><strong>Infrastructure and device risk</strong></td>
<td><strong>Financial risk</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>● Usage of untrusted devices: end-users modifying or bypassing device security controls.</td>
<td>● Increased risk of loss of value when employees bring the organisation’s brand into dispute by uncontrolled used of devices. Cost of compliance increases.</td>
</tr>
<tr>
<td>● Sophisticated and varying attack vectors targeting mobile users and devices.</td>
<td>● Data breach costs.</td>
</tr>
<tr>
<td>● Diverse mobile ecosystems can result in an expanded attack surface or enterprise risk profile.</td>
<td>● Cyber liability.</td>
</tr>
<tr>
<td>● Third party application vulnerabilities, applications and questionable motives.</td>
<td></td>
</tr>
<tr>
<td>● Lack of physical security controls (remote wipe not a universal solution as attempts frequently fail for lost or stolen mobile devices.</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Deloitte (2013:88)*

With all the threats and risks highlighted above, it is important for any organisation to clearly define the responsibility for ensuring BYOD is secured. This assist both the organisation and employees to be accountable for securing the organisation’s information. It is also important for the organisation to conduct a risk assessment to determine what threats it will be exposed to as a result of weak security controls and the level of risk that the organisation is willing to tolerate.

### 2.6 SECURING A BYOD ENVIRONMENT

Information must be protected in a manner that is commensurate with its sensitivity, value and importance. Security measures must be employed regardless of the medium on which the information is stored (paper, electronic, computer bits, etc.), processed (through a computer, mainframe, voice mail system, etc.) or moved (email, face-to-face conversation, etc.). The management of an organisation is often responsible for realising the importance of information security in their organisation, they accept the accountability and responsibility of the information governance of their organisation. Users of the system
are also responsible for the security of the organisation’s resources as part of their employment contract (Von Solms & Van Niekerk, 2013:9).

The BYOD programme should be owned by the IT department. Although every department and every employee accesses data, it is nonetheless the responsibility of the IT department to enable other departments with the necessary tools to help employees be as productive and efficient as possible, while also keeping corporate data secure. One way to do this is to make sure data deletion software is pre-installed before mobile devices are allowed to connect to the corporate network (Burt, 2011:30). Having a well-defined boundary in place should help resolve responsibilities for security within BYOD. This could also assist in addressing the conflict that most organisations face concerning accountability (Thomson, 2012:5).

Although the employee owns the device, together with the personal information stored on, there should be a policy in place that clearly states that any information that is stored on the device for work-related purposes should remain the property of the organisation (Harris, Ives & Junglus, 2012,23). The responsibility of securing organisational data becomes important especially when an employee loses their device. The protection of information should be the responsibility of all employees regardless of whether the department supports BYOD or not. This is possible with sufficient training and supporting reference materials, to allow employees to properly protect and manage the organisation’s information assets (Harris, Patten & Regan, 2013:5).

2.7 RISK ASSESSMENT PRIOR TO IMPLEMENTING BYOD

Risk management encompasses three processes, namely, risk assessment, risk mitigation and revaluation and assessment. In this study, risk assessment with regard to adopting BYOD will be examined. Risk is defined by Deloitte (2006:3) as the diminished opportunity for gain, the probability of failure or factors that can have a negative impact on the organisation’s objectives.

Most often, the definition of risk is associated with potential losses, however, it is also possible for benefits to be derived from taking risks. Olson (2002:5) defines risk as “uncertainty of future outcomes” while Lucouw (2004:80) refers to the possibility that some unknown event will happen. He then argues that risk is associated with negativity
since there is anticipation that the actual results will be worse than the anticipated outcome.

Risk assessment can be used as a means to obtain a greater understanding of any factors that could harm or have an impact on the operations of the organisation or its services, i.e IT. Risk assessments can be conducted through different levels within the organisation. These levels include Strategic, Compliance, Internal Audit, Operational, Financial Statement, Fraud Risk, Security Risk and Information Technology Risk (Atkinson & Jourdan, 2008:3).

In assessing risk associated with BYOD, the organisation needs to define the scope of the effort. Boundaries for both IT systems and devices are identified along with the resources and information to establish the system. The first step of risk assessment is to identify all potential sources of threat and compile a threat statement (Li & Clark, 2013:79). Analysing the BYOD threat to the organisation includes analysing the system environment that is impacted.

A list of vulnerabilities (weaknesses) that could be exploited by potential threat-sources should be developed as part of the risk assessment steps (Li & Clark, 2013:79). Vulnerability assessment includes testing controls that are already in place. Testing can be conducted in three ways (DeSmit, Elhabashy, Wells & Camelio, 2017: 340):

- **Automated vulnerability scanning tool**: This tool is used to scan groups of hosts or networks for any known vulnerable services such as scanning whether the stream allows anonymous File Transfer Protocol.
- **Security test and evaluation**: This is another technique that could be used to identify vulnerabilities within the organisation’s systems and devices. This includes developing and executing a test plan to test the effectiveness of the security controls within the organisation. The main purpose is to ensure that the controls that are already in place meet the approved security specifications for software and hardware and industry standards.
- **Penetration testing**: This is usually used to supplement the review of security controls and make certain that different facets of the IT system are secured.

The likelihood of potential risks materialising needs to be determined as well as the security controls that have already been implemented. It is important for an organisation
to determine what impact the risks would have on the entire organisation; this assists in prioritising the impact and levels associated with information assets being compromised based on an assessment. In addition, the following procedures can be performed as part of the risk assessment (Dawson & McDonald, 2016:52):

● The organisation must assess and document the risks associated with the internal environment including devices that are not under the organisation’s control as well as applications and data that would be exposed to threats.
● Senior stakeholders must understand the risks and benefits of having BYOD in an organisation.
● Any requirements for any technical solutions that will be chosen to facilitate BYOD should be documented.
● A network architecture review should be performed of the risk assessment process, the current architecture and the proposed architecture for BYOD. This should be done preferably by an independent and external party. This includes security controls such as firewalls which have been put in place to segregate the BYOD environment away from other critical, internal environments.
● A technical assessment should be conducted of the environment, pre-implementation, to ensure that any existing issues that that were not previously addressed are dealt with. The organisation must understand the issues associated with its internal environment now that outside devices will be brought in behind external firewalls.

Once a risk assessment has been conducted and the decision to onboard devices onto the organisation’s network has been taken, information security policies that govern mobile device should be implemented.

The next section will look at the mobile device policy or controls that should be embedded in the existing information security policy to enable the bank to address the threats and risks identified above.

2.8 MITIGATION OF BYOD IT RISK

Mobile technology is moving at a rapid pace and organisations are required to prepare for a new era of MDM. The preparation will include the development of a mobile device management policy for personal mobile devices that are used for work purposes. MDM is a critical aspect in protecting devices that are part of BYOD programme.
MDM can be used to provision the device using Over-The-Air (hereafter OTA) or other methods. The term ‘OTA’ refers to the use of wireless mechanisms to send provisioning data or update packages for firmware or software updates to a mobile device. Other forms of MDM interact with directory services such as Microsoft Active Directory (MAD) to increase visibility across the organisation. Necessary certificates should be installed on the device, configurations of the device as well as software required to enable BYOD security controls and standards. MDM will assist in supporting the mobile device by relying on complete software solutions that can be used by organisations to lock down, control, encrypt and enforce policies (Liu, Moulic & Seo, 2010:474). Figure 3 below shows the architecture of MDM and illustrates how it operates.

![Figure 3: MDM architecture](image)

Source: Ghosh, Gajar & Rai (2013:66)

The architecture depicted in Figure 3 shows mobile devices connected to the organisation’s network via an encrypted channel. MDM is placed in the Demilitarised Zone (DMZ), sometimes referred to as the ‘perimeter network’. DMZ is a physical or logical sub-network that contains and exposes an organisation’s external facing services to an untrusted network. DMZ is public-facing so that mobile devices which are trying to communicate from the external network can be enrolled and configured by the MDM (Al-Nashif, Chadaga, Cox, Hariri & Mallouhi 2011:1).
Policies can be enforced, and activities monitored. By implementing the BYOD policy, employers will be able to control what resources are available to the employees and prioritise delivery of information based on the user’s need (Dahlstrom & diFilipo, 2013:15). The BYOD policy will also provide the organisation with more systematic and integrated procedures for managing threats, maintaining the mobile devices and dealing with any legal implications that may arise (Dhingra, 2016:184). The importance of having BYOD policy is discussed in greater detail in the section below.

2.8.1 Mobile device policy

In the previous section, the importance of conducting a risk assessment before implementing BYOD was addressed. This is to ensure that both employee and employer assets are protected. This is especially important in the financial services industry since which well known for its complexity, risk and increasingly high requirements for information privacy. Access and disclosure of financial and personal information is highly regulated and failure to comply with regulations comes with potential large fines (IDC, 2015:1).

This section discusses the importance of having a mobile device policy or embedding controls in the existing information security policy. These will ensure that risks are accounted for and managed appropriately. The organisation should first decide on the scope of the policy and determine what kind of mobile devices employees are using for work purposes. Then the organisation can decide which type of device to include under the policy and clearly communicate which devices it will and will not support, including the information that will be permitted to be accessed through those devices (Shahbazi, 2014:20).

It is important for the BYOD policy to address the constraints of access control and protection of organisational information resources by both internal and external users (Keyes, 2013:233; Caldwell, Zeltmann & Griffin, 2012:1). BYOD policy will assist the organisation in ensuring risks and controls are accounted and managed appropriately. BYOD policy can be described in three layers operational, tactical and strategic as illustrated in Figure 4 below.
Figure 4: BYOD policy architecture

*Source*: Bais (2016:193)

The operational layer of the architecture refers to the core regulation of BYOD devices and users and operates in conjunction with the other two layers (tactical and strategic). The tactical layer supports the information security of the organisation as well as its privacy while the strategic layer covers risk management and governance aspects of BYOD (Bais, 2016:194). These three layers and underlying principles are presented in detail in Table 2 below.
<table>
<thead>
<tr>
<th>Table 2: BYOD environment architectural principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. On-boarding of the devices</strong></td>
</tr>
<tr>
<td>The objectives of this principle are to determine responsibilities of on-boarding mobile devices, including types of mobile devices that are permitted to access the organisation’s network. These also include the number of mobile devices an individual is permitted to onboard.</td>
</tr>
<tr>
<td><strong>1.1 User Account Registration</strong></td>
</tr>
<tr>
<td><strong>Control:</strong></td>
</tr>
<tr>
<td>Employees should provide verifiable information about themselves such as employee user ID, their role and department to create an account and register their mobile device.</td>
</tr>
<tr>
<td><strong>1.2 Device Registration</strong></td>
</tr>
<tr>
<td><strong>Control:</strong></td>
</tr>
<tr>
<td>Employees should provide information about their mobile devices such as make/model, serial number, IMEI number and MAC address</td>
</tr>
<tr>
<td><strong>1.3 End-user/Service Agreement</strong></td>
</tr>
<tr>
<td><strong>Control:</strong></td>
</tr>
<tr>
<td>Employees must agree to a set of requirements concerning the usage of information resources and liabilities that will emerge as a result of the mobile device and data being stolen or lost.</td>
</tr>
<tr>
<td><strong>2. Identification &amp; Access Control in the Policy</strong></td>
</tr>
<tr>
<td><strong>2.1 Password:</strong></td>
</tr>
<tr>
<td>The objective of enforcing strong password is to protect unauthorised access to the mobile device and organisation’s network.</td>
</tr>
<tr>
<td><strong>Repeated and Sequential Characters</strong></td>
</tr>
<tr>
<td><strong>Control:</strong></td>
</tr>
<tr>
<td>Restrict employees from using repeated or sequential characteristics in their password.</td>
</tr>
<tr>
<td><strong>Alphanumeric values, peer/lower case characters and special characters</strong></td>
</tr>
<tr>
<td><strong>Control:</strong></td>
</tr>
</tbody>
</table>
Password should contain both upper and lower case characters and have at least two letters, one number and one special character such as & ! #

**Password length**
*Control:*
Password must be a least 8 characters long

**Password age and history**
*Control:*
Passwords should be changed on a regular basis. The new password should not be accepted if it matched three previous used passwords by the same employee.

**Auto Lock (in Minutes)**
*Control:*
Device auto lock should be set to 3 minutes. If the device is not used for the specified period of time, it automatically locks within 3 minutes.

### 2.2 Authentication
The objective is to identify and verify BYOD users and the devices

**Multi-factor authentication**
*Control:*
To prevent the mobile device from unauthentic users or from unwanted access, the user should use trusted signed digital certificates or use a digital signature algorithm. The two above can be exchanged between the mobile device and organisational systems to authenticate.

### 2.3 Authorisation
The objective of authorisation is to ensure employees and mobile devices are granted different access rights to organisational systems and resources.

**Access Privileges**
*Control:*
Mapping confidential information resources to the right mobile device should occur within the context of authentication. Rules must be implemented to determine the kinds of activities the employee or mobile device is permitted to access and use.

**Network Segregation:**
The objective of segregating the network is to ensure that access to sensitive information is minimised.

**Guest / BYOD Users’ Network**
*Control:*
The key organisational network should be partitioned into smaller networks to develop and enforce a rule set that controls which employee and mobile devices are permitted to communicate with the organisational systems.

3. Communication Policy

Data Protection

3.1 Encryption

The objective is to protect confidential information that belongs to the organisation on mobile devices.

Device Internal Memory Encryption

Control:

Encryption algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES) or Blowfish should be used to protect email and text messages, contact lists, calendars and other credential information on the mobile device.

Device External Memory Encryption

Control:

Encryption applications should be installed on the mobile device to protect all information stored in removal/flash memory cards.

3.2 Virtual Private Network (VPN)

The objective of VPN is to ensure that the integrity of the data is preserved during any communication.

VPN Applications and Settings

Control:

Mobile VPN and other VPN application controls should be used to maintain information in transit accuracy during data exchange and communication between mobile devices and organisational applications.

3.3 Data Wiping

The objective of wiping data that resides in the mobile device is to preserve the confidentiality of information when the mobile device is lost or stolen.

Remote Wipe

Control:

IT administrators should be able to remotely wipe lost or stolen mobile devices with the full consent of the owners/users or in accordance with the end-use/service agreement that was completed when the mobile device was onboarded.

Selective Wipe
**Control:**
IT administrators should be able to selectively wipe organisational information off the mobile devices that are infected or highly vulnerable to malware/viruses or if the employee has violated control measures set in the policy.

**Device Auto Wipe**

**Control:**
Employees and IT administrators should be able to activate automatic built-in device wipe features installed, after a series of failed password attempts.

### 3.4 Data Backup
The objective of backing up data is to maintain the availability of the employee’s personal information in the event of device/data loss or corruption.

**Encrypted Backup Service**

**Control:**
Data on mobile devices should be backed up regularly, either remotely via the internet or through cable, using encrypted data backup software and services.

### 3.5 Device Lockdown
The objective is to lock down the mobile device remotely when it is lost or stolen.

**Device Lockdown Software**

**Control:**
IT administrators and BYOD users should use applications to remotely lock or shut down compromised devices.

### 4. Application Control Within the Policy

#### 4.1 Trusted and Verified Apps
The objective of this control is to ensure that applications installed on the mobile device are verified and trusted is to avoid the installation and usage of uncertified applications.

**In-house IT Applications**

**Control:**
All in-house applications developed for the mobile device should be certified by the IT stakeholders.

**Applications Testing and Deployment**

**Control:**
All applications should be tested by the organisation information security team, followed by approval from executive management before usage in the mobile device.

**Third Party and External Control:**
Employees should only install code-signed applications by developers.

4.2 Licensed and Curated Application Stores
The objective is to avoid the installation and usage of malware applications on BYOD devices.

**Secured Application Stores Control:**
Employees should download and install applications from organisational IT services where applications will be thoroughly tested before being made available for commercial download.

4.2 Blacklisting and Whitelisting Applications
Blacklisting and whitelisting application controls are used to ensure that uncertified and malicious applications are identified.

**Applications Blacklisting Control:**
All malicious and untrusted applications should be securely removed from the mobile device and blacklisted so that they cannot be installed on the device or be operable on organisational systems and network.

**Applications Whitelisting Control:**
A list of trusted and certified applications should be maintained to eliminate the risk of installing unknown or unwanted applications on mobile devices.

4.5 Virtualisation:
Virtualisation prevents unauthorised manipulation of organisational data by the mobile device.

**Virtual Desktop Infrastructure Control:**
Desktop virtualisation should be employed for executing applications and storing data rather than from the mobile devices.

**Strategic layer**
5.1 Risk Control Policy

Malware Prevention

Malware prevention control assists in protecting and preventing the mobile device and organisational resources from malware attacks.

**Anti-Virus/Anti-Malware Programme Functionality**

*Control:*

In addition to protecting mobile devices and applications on it, anti-virus and anti-malware programmes should be able to scan the device thoroughly to detect and remove latest viruses, Trojan horses, worms, Adware, spyware and rootkits.

Firewall Programmes

Firewall programmes block inbound and outbound malicious connections and filter traffic demands of mobile devices and applications.

**Firewall Programme Functionality**

*Control:*

In addition to blocking network traffic from suspected malicious source, the firewall should be able to filter and restrict mobile device access based on network type, applications type and other packet attributes such as IP address.

5.2 Intrusion Detection Prevention

The objective is to detect or prevent unauthorised access and attacks from mobile devices.

**Intrusion Detection System**

*Control:*

Network access points for mobile devices should be integrated with intrusion detection systems to act as a security sensor that can identify and stop unauthorised access and threats from compromised mobile devices.

5.3 Awareness and Training

Awareness and training is important to educate employees on how to avoid threats and vulnerabilities when using their mobile devices as well as comply with organisational BYOD policy.

**Computer-based Training Workshop**

*Control:*

All employees in the organisation should regularly attend online and distance training programs about current and future potential risks in BYOD environments and how they can be mitigated.

**Instructor-based Training Workshop**
Control:
All employees should regularly engage in face-to-face training programmes in order to increase their focus on threats and vulnerabilities and establish dialogues with instructors on mitigation strategies.

6. Compliance Policy
6.1 Security/Privacy Principles and Laws
The objective of having compliance in BYOD policy is to ensure that the organisation complies with information security and privacy standards and abides by national principles and laws with regards to information protection.

Complying with National Information Security and Privacy Laws
Control:
Security and privacy policies should be developed, modified or updated according to specific country laws or the region in which an organisation operates.

Complying with Information Security and Privacy Standards
Control:
In addition to compliance with information security and privacy standards, the standards should be adapted to accommodate and manage BYOD.

6.2 Employee Privacy Considerations
The objective is to maintain the privacy of employees’ personal data

Data Collection Limitation
Control:
Employees’ personal data should only be obtained in a legal and fair manner with the knowledge/consent of the data subjects.

Purpose Specification of Data Access and Collection
Control:
Employees’ personal data access and collection by organisations should only be carried out when there is a satisfactory warrant in accordance with the authority of law.

Data User Limitation
Control:
Employees’ personal data should not be disclosed or used for other purposes other than those specified in the end-user/service agreement or except with the permission of the data owners.

Individual Participants
Control:
Employees should be allowed to challenge any data collected related to them, to either be erased or amended.

Technical Safeguards

*Control:*

Reasonable techniques that involve disk partitioning or ‘containerisation’ and virtualisation should be used to segregate employees’ personal data and organisational data to allow selective wipe of data when employees leave the organisation or mobile devices are lost or stolen.

7. Maintenance Policy

7.1 Internal and External Systems/Devices Update

The objective is to improve infrastructure of organisations and mobile devices used for work purposes.

Updating Control Systems and Devices

*Control:*

Organisations’ infrastructure and mobile device operating systems and applications should be regularly updated to resolve security vulnerabilities and threats as well as provide performance options and features to users.

7.2 Policy Review and Update

The objective is to assess BYOD policy and ensure that the policy is up to date.

Review and Updating Policies

*Control:*

BYOD policy should be reviewed and updated regularly to ensure adequate control measures that are compliant with regional laws, are in place and can cope with the continuous demands of BYOD.

Source: Ghosh et al. (2013:66) & Bais (2016:193)

**Summative comment**

As stated above, effective BYOD policy provides IT departments with a clear view of risks and controls that should be in place when employees are allowed to use their personal mobile devices for work purposes. The controls formulated above will guide the banking environment in managing mobile device risks properly.

2.9 CRITICAL LINKS TO THE EMPIRICAL RESEARCH
A BYOD policy is one of the key strategies to address IT risk that banks may encounter as a result of allowing employees to use their own mobile devices for work purposes. It is important for the bank to have a BYOD policy considering the amount of client data they hold within their organisation. In this study, the BYOD policies of the four major banks in South Africa were evaluated through an empirical study which:

- Evaluated whether information security policies of the big four banks include the seven principles of BYOD policy as stated above. This was done through a questionnaire (Onboarding, Identification & Access Control, Communication, Application Control, Risk Control, Compliance and Maintenance).
- Determined whether the banks fully understood the impact of BYOD on their organisation.

2.10 CONCLUSION

This chapter provided a background of BYOD, its definition and its characteristics. The chapter also provided insight into the benefits of BYOD such as affording employees the flexibility of working anywhere and at any time, cost reduction of maintaining the devices, and the like. The defining characteristic of BYOD include mobility, mobile environment, mobile technology, mobile computing and consumerisation. Although there are many benefits of BYOD, there are also a number of challenges which need to be addressed to ensure that the organisation continues to operate effectively and ultimately achieves its goals. Key threats are mobile device malware, mobile devices being lost or stolen and malicious insiders trying to sabotage the organisation.

Key risks such as operations, legal and regulatory risk, infrastructure and device risk and financial risk that may hinder the organisation to operate effectively were also discussed in brief. It was noted that responsibility for the security of BYOD lies with both the employer and the employees who are using their device for work purposes.

In any business, risk assessment is important in identifying the risks the organisation is likely to encounter and how these will impact the organisation if proper controls are not in place. Risk assessment also assists in designing controls to mitigate the identified risks. In this study, mitigating controls were discussed as part of BYOD policy.
In conclusion, the importance of implementing a BYOD policy were discussed. BYOD policy can be designed in three layers (operational, tactical and strategic). These can be further broken down into seven principles: Onboarding, Identification and Access Control, Communication, Application Control, Risk Control, Compliance and Maintenance). These seven principles were assessed through a questionnaire on the BYOD/mobile device policy of the four biggest commercial banks in South Africa. The research methodology and approach to the empirical research are discussed in the following chapter.
CHAPTER THREE: RESEARCH METHODOLOGY AND DESIGN

3.1 INTRODUCTION

The literature review in Chapter Two provided the context of the study based on relevant research on IT risk stemming from the use of personal mobile devices for work purposes. The benefits and challenges of BYOD were discussed to emphasise why organisations are adopting BYOD and the importance of having a policy in place to mitigate BYOD IT risks. Chapter Two set out the responsibilities of managing BYOD and conducting the risk assessment before adopting BYOD. Lastly, there was a detailed discussion of the seven security principles that should be in place in a BYOD policy to address some of the risks resulting from BYOD.

Chapter Three address the research methodology used in the study to respond to the research objectives outlined in section 1.3. This chapter also discuss the research design and the research approach which were used to determine whether the information security policies and the mobile device policies of the big four commercial banks of South Africa covered the seven key security principles as stated in Chapter Two.

3.2 RESEARCH DESIGN

The term ‘research design’ takes on different meanings in different studies. For instance, in one study, research design may reflect the entire research process, from conceptualising the problem, to the literature review, the research questions, method and conclusion (Bordens & Abbott, 2002:16), while in another, research design may refer only to the methodology of a study. Research design is further defined by Burns, Grove and Gray (2012:195) as the “Blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings”.

Collectively, research design can be defined as plans and procedures that cover all the study decisions, from the broad assumptions to the detailed methods of data collection and analysis. This empirical part of this study will be conducted through a questionnaire based on the literature review. The questionnaire was designed to evaluate whether BYOD’s seven security principles and controls were applied properly in the sample of banks tested. The method of how this research was conducted is discussed below.
3.3 RESEARCH METHODOLOGY

According to Kumar and Phrommathed (2005:23), a research methodology is a theory of how an enquiry should proceed. An enquiry involves analysing assumptions, principles and procedures. Burns, et al (2011:223) define a research methodology as the total strategy that stems from identifying the problem to gathering and analysing the data. Leedy and Ormrod (2001:66), on the other hand, define research methodology as “the general approach the researcher takes in carrying out the research project”. There are three types of research methodology that a researcher can adopt, namely, qualitative, quantitative and mixed methods. In this study, both qualitative and quantitative methods were adopted.

3.3.1 Research approach

In order to respond to the research questions stated in section 1.3.2, both qualitative and quantitative methodology methods were used.

Qualitative research has a multi-method in focus, involving an interpretive and naturalistic approach to the subject matter. This approach involves questions and procedures, data is typically collected in the participant’s setting, data analysis inductively extrapolates from the particular to the general and the researcher interprets the meaning of the data (Riley & Love, 2000:166). A qualitative approach was used in this study to provide credible, accountable and legitimate answers to the research objective.

Rubin and Rubin (2011:10) define quantitative research as an approach which aims to develop theories and understanding. Denzin and Lincoln (2011:10) add that quantitative research is an approach that enables the user to be more efficient while at the same time remaining objective. A quantitative approach was used in this study to evaluate mobile device policies of the big four commercial banks in SA through a questionnaire, with the aim of determining whether mitigation policies were adopted to address BYOD IT risks.

3.4 POPULATION AND SAMPLE

Polit and Beck (2004:50) define a population as the aggregate or totality of those conforming to a set of specifications. Due to the large size of populations and the
limitations of resources, it is generally not possible to evaluate an entire population. In such cases, a sample of elements is evaluated.

The target population of this study was financial institutions, and specifically, banks, which were chosen due to the pivotal role they play in modern economies. Banks remain one of the key financial intermediaries in an economy, providing a variety of services. The efficiency of financial intermediaries can have a significant impact on the economy. Banks also contribute to the monetary policy of South Africa.

The study population was extracted from commercial banks in South Africa. According to Buzz South Africa (2018:1), there are 17 commercial banks in the country. This study only considered the four major banks based on their asset size. These banks were Absa, FirstRand, Nedbank and Standard Bank.

A sample is defined by Polit and Beck (2004:731) as a selected portion of the population that conforms to a designated set of specifications to be studied. The banks sampled in this research are the four major commercial banks in South Africa. The study examined data for a period of 12 years, from 2005-2018. This was to ensure that the assessment of BYOD IT risks and associated controls was thoroughly evaluated and to observe how the risks and controls matured over the period of 12 years.

The banks chosen for the sample represented 85% of the banking market share. According to Business Technology (2018:1) and Relbanks (2018:1), Standard Bank, FirstRand, Absa Group and Nedbank were the four biggest commercial banks in 2018 based on total assets, as indicated on Table 3 below. The research considered certain criteria which included professional expertise and readiness to take part in the research.

Table 3: Sample selected

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Bank</th>
<th>Year Established</th>
<th>Total Assets (R mil)</th>
<th>Head Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standard Bank</td>
<td>1962</td>
<td>254 849</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>2</td>
<td>First National Bank</td>
<td>1929</td>
<td>120 747</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>3</td>
<td>Absa</td>
<td>1991</td>
<td>983 378</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>4</td>
<td>Bank Nedbank</td>
<td>1888</td>
<td>892 006</td>
<td>Johannesburg</td>
</tr>
</tbody>
</table>

Source: Business Technology (2018:1)
A purposive sampling method was used to determine the number of participants who would be given the questionnaires. Barrios and Guarte (2006:277) describe purposive sampling as a method of randomly selecting a sampling unit within a population with the most information on the subject under investigation. The following criteria was used to select participants to conform to the objective of the research and to reduce disparity amongst participants.

- The participants had to be responsible for the IT governance policy of the organisation.
- The participants had to have professional expertise in IT risk and information security.

3.5 RESEARCH INSTRUMENT

The questionnaire comprised of open-ended and closed-ended questions. Open-ended questions are designed to ensure that participants have the opportunity to state their views freely without being influenced while closed-ended questions limit participants to a number of alternatives (McCawley, 2009:13). The questionnaire was formulated to elicit relevant data on the impact of BYOD risks on the banks’ information technology assets. The open-ended questions were informed by the literature review in Chapter Two and consisted of the security principles that should be addressed by the information security / mobile device policy to ensure effective control of mobile devices.

The questionnaires were completed by one representative for each of the four banks. These representatives were heads of IT governance and were responsible for developing, implementing and maintaining the policies, systems and procedures for the management of information throughout its life cycle. The participants were selected because of their comprehensive knowledge of IT risk and security controls.

The questionnaires were sent by email to the participants. The content of the questionnaires was as follows:

- **Question 1**

  **Objective:** To determine whether a policy is in place to ensure that the bank complies with information security and privacy standards and abides by the principles and laws of information protection.

  Q: Do you have a mobile device policy in place?
• **Question 2**  
  **Objective:** To determine whether employees’ mobile devices were on-boarded prior to accessing the organisation’s network.  
  Q: How are employees’ personal mobile devices on-boarded to the organisation’s network?

• **Question 3**  
  **Objective:** To ensure that training and awareness is provided to employees before they are allowed to access the organisation’s network to ensure awareness of threats and vulnerabilities.  
  Q: Do you offer training to employees prior to on-boarding? If yes, what kind of training is offered?  
  Q: How do you ensure all employees in the organisation are aware of the mobile device policy?

• **Question 4**  
  **Objective:** To determine if there are any IT threats and risks that the banks are concerned about.  
  Q: What are the major IT risks that the organisation is exposed to when employees make use of their personal devices for work purposes?

• **Question 5**  
  **Objective:** To determine whether the organisation allows employees to download external applications onto BYOD devices.  
  Q: Do you allow employees to download external applications that are not approved by the organisation onto their personal devices?

• **Question 6**  
  **Objective:** To evaluate whether the bank has experienced incidents as a result of BYOD and to determine whether effective controls have been implemented to mitigate the risks they are concerned about.  
  Q: Have you had any incidents of data breach as a result of employees using their personal devices for work? Please provide an example of such a data breach.  
  Q: Do you believe that the controls your organisation has implemented are effective to mitigate the risks the bank is concerned about?
Q: Please describe the controls that the organisation has implemented to mitigate the risks that emanate from this and how do you control these risks?

- **Question 7**
  
  **Objective:** To determine whether the bank maintains the privacy of employees' personal information and what controls have been implemented.

Q: Do you have controls in place to ensure that the privacy of employees' personal information contained on their mobile device is maintained? If yes, what controls have you implemented?

- **Question 8:**
  
  **Objective:** To determine whether the policy and the bank's infrastructure are updated on a regular basis to cater for emerging threats and risks of mobile devices.

Q: How often is the policy updated?
Q: Are the bank's infrastructure and mobile device operating systems and applications regularly updated to address security vulnerabilities and threats?
Q: Do you believe the policy had added benefit in how the organisation manages risks? If yes, what kind of benefit has the bank derived?

Further, all the questions were designed in a manner that the participants could easily understand them. The questionnaire was reviewed by the ethics committee and ethical clearance was obtained. A copy of the questionnaire is included as Annexure 2.

### 3.6 DATA ANALYSIS AND INTERPRETATION

Data collection is defined by Burn and Grove (2011:460) as the process of selecting participants and gathering information from them. Data analysis consist of three steps, namely, evaluation, presentation and conclusion. In this study, the results of the questionnaire were interpreted and linked to the seven security principles that were discussed in Chapter Two.

### 3.7 VALIDITY AND RELIABILITY

Validity is defined by Macmillan and Schumacher (2001:40) as the degree to which the interpretations and concepts have mutual meanings between the participants and the
researcher. Reliability is defined as the degree to which the findings are independent of accidental circumstances (Silverman, 2016:215).

Validity in this study was ensured by employing a qualitative research approach. This approach allowed the contents of the information security / mobile device policies to be analysed through structured principles as defined in section 3.5. A structured questionnaire was developed from the literature review in Chapter Two.

Reliability is defined by Zikmund, Carr and Griffin (2010:302) as an indicator that measures internal consistency. McDaniel & Gates (2004:203) state that it is necessary to determine whether the questionnaire measures what it is intended to measure. One random bank was selected to test the reliability of the questionnaires. Any suggestions or problems were identified, and the questionnaire were slightly adjusted accordingly. Therefore, the test-retest method was utilised.

3.8 ETHICAL CONSIDERATIONS

The University of Johannesburg’s ethics committee reviewed the questionnaire and clearance was obtained. The participants were requested to read and sign an Informed Consent Form. Participants were informed of the confidentiality clause when analysing the IT security policies. Confidentiality implies that the dignity of the subject shall be respected; therefore, it was important that the participants had no doubt that any identifying information would be regarded as confidential. The identity of the participants thus remained anonymous by using a letter to identify the banks, for example: Bank A, B, C and D.

In terms of citations of other authors, credit was given where it was due by using the Harvard referencing technique and the work of others was not misused in any way.

3.9 CONCLUSION

This chapter described the research design that was adopted to address the research objectives stated in Chapter One. The study followed a mixture of qualitative and quantitative methodology to achieve the research objectives. This chapter outlines the steps followed to conduct the research. It was explained that primary and secondary data
would be used to address the research problem. The primary data was represented by the literature review while secondary data were represented by the questionnaire. The population together with the sample consisting of financial service providers in South Africa was discussed in detail. The sample was based on the top four commercial banks based on the assets value they hold deemed to be a representation of all the banking industry in South Africa.

Validity and reliability can only be determined once the results of the big four commercial banks are analysed. Further, this chapter also addressed ethical considerations to ensure that the rights of the organisations were protected. An evaluation of IT risks as a result of the use of personal mobile device for work purpose is deemed necessary to determine what risks are the organisations exposed to and assess whether there is a policy in place that governs controls round BYOD.

The next chapter will concern the empirical study and the results obtained from the empirical study
CHAPTER FOUR: RESEARCH FINDINGS AND ANALYSIS

4.1 INTRODUCTION

BYOD has positively influenced the banking environment. Banks understand that in order to grow their business, technology is one of the main driving forces. BYOD benefits were highlighted in detail in section 2.4 of the literature review. These benefits include, but are not limited to, employees being able to work from anywhere at any time using their personal mobile devices, enhanced productivity and cost savings to the employer. Although there are numerous benefits of BYOD, there are also challenges introduced to both the organisation and its employees.

The most common challenges include malicious software that can infiltrate the organisation's hardware and software through the network, unauthorised access to data through weak security controls on the mobile devices, mobile devices that are lost or stolen or unauthorised individuals gaining access to the data on the device. At the same time, a balance must be maintained between the security of the organisation on the one hand, and the privacy of employees on the other. These challenges have motivated the development of mobile device policies and guidelines.

It is important to investigate the beliefs and practices that the banks have adopted to manage IT risks stemming from BYOD. The study focuses on the adoption of BYOD, its associated risks and the controls implemented to mitigate it. The study also investigates whether IT controls have been adopted effectively to mitigate both IT risks and any privacy concerns within the BYOD environment.

The banks' mobile device policies and other procedures that address BYOD IT risk were evaluated. This chapter presents the results and analysis of the data that was obtained from the questionnaires. The method of how the questionnaire was designed and objectives are discussed below.

4.2 QUESTIONNAIRE RESPONSE RATE

The questionnaire was completed and returned by way of email and a 100% response rate was obtained.
Table 4: Response rate

<table>
<thead>
<tr>
<th>Questionnaire to the SA four major banks</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No response</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Completed and usable questionnaire</td>
<td>4</td>
<td>100%</td>
</tr>
<tr>
<td>Total percentage of questionnaires sent out</td>
<td>4</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.3 RESEARCH PARTICIPANTS

The participants’ total years of experience ranged from 6 to 14. Participants were selected because of their comprehensive understanding of IT security controls and risks. Based on their experience levels and position in the bank, the sample appears to be appropriate for the study. The position and years of experience of the participants are provided in Table 5 below.

Table 5: Research Participants

<table>
<thead>
<tr>
<th>Sample Bank</th>
<th>Position</th>
<th>Approximate years of experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Senior Officer: Risks and Controls</td>
<td>6 to 14 years</td>
</tr>
<tr>
<td>B</td>
<td>Chief Information Officer</td>
<td>6 to 14 years</td>
</tr>
<tr>
<td>C</td>
<td>Head of Information Risk</td>
<td>6 to 14 years</td>
</tr>
<tr>
<td>D</td>
<td>Head of Information Risk and Governance</td>
<td>6 to 14 years</td>
</tr>
</tbody>
</table>

4.4 RESEARCH FINDINGS

The responses of the banks to the questionnaire are analysed in the following sections.

4.4.1 Do you have a mobile device policy in place? And do you believe the policy has added benefit in how the organisation manages risk?
Figure 5 below presents the percentage of the sampled banks that have implemented a mobile device policy and benefited from having such a policy in place.

![Pie chart](image)

**Figure 5: An overview of mobile device policy usage across the sample banks**

The results indicate that all of the sampled banks have implemented a mobile device policy and are realising the benefits of having such a policy in place. A mobile device is described in section 2.4 as one of the core drivers that increases productivity as it means employees are not restricted to one workstation. Employees are able to work from anywhere at any time, using their personal mobile devices. Organisations have become more aware of benefits such as the policy enabling the implementation of controls, employees' awareness of the IT risks, improved compliance with privacy acts, decreased severity of data breaches and employees understanding the risks and controls that need to be implemented to ensure that the organisation does not endure any losses.

Section 2.8.1 introduced mobile device policies as one of the mitigating factors for the risks that BYOD may introduce to the organisation. A mobile device policy outlines practices and requirements for the use of mobile devices and applications. The policy also reminds employees of the organisation’s values and mission by tabling some of the threats that the organisation may encounter as well as how the organisation is expected to respond.

**4.4.2 How often is the policy updated?**
Figure 6 below presents the frequency at which the sampled banks update their mobile device policies. The results indicate that 75% (3/4) of the banks update their policy on an annual basis while 25%(1/4) do so every two years, unless new information comes to light. Then the policy is updated immediately.

![Frequency of updating the policy](chart)

**Figure 6: Analysis of how often banks update their mobile device policies**

As can be seen from the responses above, three of the four banks ensure that their policies are updated on an annual basis. Only one institution updates its policy every two years.

A mobile device policy should be regularly maintained to improve the organisation’s infrastructure. Section 2.8.1 and the research findings in the preceding section affirm the importance of maintaining a mobile device policy to ensure that adequate IT control measures are in place and to provide guidance on how information should be handled and protected. Of the sample, three of the banks responded appropriately to the changes in BYOD and its associated risks, by regularly updating their policy. The bank which only updated its policy once every two years should consider a more regular update to ensure that the policy addresses all risks that arise as a result of using mobile devices for work purposes as risks evolve rapidly, in step with advances in technology.

4.4.3 Are employees’ personal mobile devices on-boarded onto the organisation’s network?

Figure 7 below presents the results of the sampled banks that have on-boarded their employees onto the organisation’s network. The results indicate that only 25% (1/4) of
the participants allowed personal devices to connect directly to the organisation’s network. Employees were required to sign a mobile device on-boarding disclaimer to ensure that they were aware of security threats prior to being on-boarded. On the other hand, 75% (3/4) of the banks allowed employees’ mobile devices to connect to the organisation’s mobile Wi-Fi to access emails and internet only; employees were not allowed to directly access the organisation’s network.

![Figure 7: Analysis on whether employees are on-boarded onto the organisation's network](image)

Some of the challenges that the organisation may encounter because of IT control gaps in the organisation’s network were described in section 2.5. Such challenges can occur when an employee is granted privileged access to sensitive information on the organisation’s network or when devices are not patched for security threats and expose the organisation to cyber-attack.

It is important that when the organisation decides to enable BYOD that proper risk assessment procedures are conducted, the responsibility for BYOD security is properly defined and effective security controls are designed to address any challenges.

**4.4.4 Do you offer any training to employees prior to on-boarding their device and if yes, what kind of training do you offer?**

Figure 8 below shows the percentage of the sampled banks that offer mobile device training and awareness to their employees. The results indicate that 75% (3/4) of the
banks provide training to employees when they are on-boarded onto the organisation’s network. The training is not restricted to the type of device an employee possesses; all devices are included, whether mobile devices or personal laptops.

Figure 8: Analysis of training and awareness offered to employees

The training also covers the protection of information, irrespective of whether this information is on devices that are owned by the organisation or the employees’ own devices. The training offered is part of the mandatory compliance training that employees usually complete on an annual basis. The training mainly focuses on the protection of the organisation’s information assets from any device and provides guidelines on how to protect these assets. Twenty-five percent of the sampled banks did not offer training to their employees, but employees did sign a mobile device on-boarding disclaimer prior to being on-boarded to ensure that they were aware of any security or information risks that may arise because of BYOD.

Section 2.6 described that the responsibilities of securing BYOD lay with both the employee and the employer. It is important that employees are aware of the benefits that BYOD introduces, the challenges that could arise as well as procedures to mitigate or avoid IT risks arising from BYOD. Providing proper training to employees ensures that they gain a proper understanding of BYOD IT risks such as unauthorised access to their mobile devices or malware. It also ensures that they are aware of controls and procedures that can be taken to avoid or mitigate risks.
4.4.5 What are the major IT risks that your organisation is exposed to when employees use their personal devices for work purposes?

The results indicate that all of the sampled banks were concerned about data leakage, malware, vulnerability and other viruses such as phishing. All of the banks were aware of the threats that could have an impact on the organisation such as financial risk or reputational risk as part of their day-to-day operation of the business.

Section 2.5 defined some of the IT risks that the organisation could be exposed as a result of BYOD while section 2.8 highlighted procedures that organisations can follow to address these challenges. Security remains the biggest challenge to any organisation, irrespective of whether BYOD is adopted or not. Section 2.4 further describes the main challenges as being confidentiality, integrity and availability of the organisation’s data. Three major threats (malware, malicious insider actions and loss or theft of devices) associated with BYOD were also discussed.

Section 2.5.1 explained that malware was currently the biggest mobile threat that directly or indirectly affects organisations. This threat usually results from the loss or theft of devices, which poses the risk of unauthorised individuals gaining access to the organisation’s sensitive information. Malicious insider actions were also listed as one of the major threats. This refers to individuals with access to the organisation’s network. These perpetrators can easily gain access to sensitive information or applications at any time with the intention to steal or destroy, without being suspected or detected.

4.4.6 Do you allow employees to download external applications that are not approved by the organisation onto their personal devices?

The results indicate that none of the sampled banks restrict employees from downloading any external applications onto their personal devices. This is mainly due to the banks not having full control over the device that is personally owned by the employee.

As part of on-boarding employees to the organisation, employees sign a contract that includes device management policies and procedures to protect information that belongs to the organisation from any device. Section 2.8.1 specified that mobile device applications that can be downloaded freely or open-sourced introduce IT risks to both the mobile device and the organisation. These risks include malware and viruses on the
mobile device, specifically when security controls are not configured on the device. Due to technical issues, sloppy coding, fewer security layers, no encryption-decryption systems on the device, sensitive information on the device, it is at risk for cyber-attack.

IT applications might leak confidential data to unauthorised individuals. Some of the external applications share contacts with third parties while others can go to the extent of gaining control over the user’s device and misuse personal or even organisational information.

All the participants described the risks of downloading unauthorised external applications onto the organisation’s devices in their policy and took into account data leakage as some of the risks they mentioned in question 4.5.5 above.

4.4.7 Have you had any incidents of data breach as a result of employees using personal devices for work?

Figure 9 below represents the percentage of the sampled banks that encountered IT risk incidents because of BYOD. The results indicate that only 25% (1/4) of the sampled banks had an incident where an employee who left the employment of the bank, took the organisation’s data with them on their personal device.

![Figure 9: Analysis of incidents suffered because of BYOD](image)

The incident that the one bank suffered became a threat as the data was not remotely wiped from the employee’s personal device. Confidential information contained on the device was then potentially exposed to a hacker or unauthorised persons could have used
the information for malicious activities. The remaining 75%(3/4) of the banks had not experienced incidents related to BYOD. The responsibility of ensuring that the organisation’s data that is stored on the personal devices rests primarily with the employee.

4.4.8 Describe some of the controls that the organisation implements to mitigate the risks that emanate from BYOD and how do you control these risks?

Table 4.3 below present some of the controls the sampled banks have implemented to address IT risks because of BYOD. The results indicated that 25% (1/4) of the sampled banks did not describe the controls that they have implemented to address the IT risks presented by BYOD. While 75% (3/4) of the sampled banks believe that the controls they currently have in place are effective to address IT risks, these controls include encryption (Access Control), data wiping, backing up organisational data and training and awareness sessions that are provided to the employees.

Table 6: Analysis of controls the banks have implemented

<table>
<thead>
<tr>
<th>Sampled Bank</th>
<th>Access Control</th>
<th>Back Up</th>
<th>Segregated Network</th>
<th>Data Wiping</th>
<th>Training and Awareness Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank A</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bank B</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bank C</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bank D</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Section 2.8 described some of the IT controls that organisations can adopt to mitigate IT risks introduced by BYOD. Section 2.6 discusses the importance of defining clear responsibility for managing BYOD from the infrastructure, device and data that is stored on the device. The results indicate that all the banks have clearly defined responsibilities for BYOD security, from all three levels: infrastructure, device and data management.

The participants assumed the responsibilities for BYOD security from the infrastructure level, working closely with businesses which were the custodians of data management and employees, as the owners of the device. Once responsibilities were clearly defined, controls were implemented in the form of a mobile device policy that tabled different controls. The importance of having a mobile device policy and controls was discussed above in question 4.4.1. This policy outlines controls such as identification and access
controls, blacklisting or whitelisting the device, malware prevention, awareness and training that should be provided to employees and maintenance of the device.

A distinction can be made between information that belongs to the organisation and private information that belongs to employees. However, none of the banks mentioned how they protected private data belonging to the employees.

4.4.9 Do you believe that the IT controls that your organisation has implemented are effective to mitigate the risks the bank is concerned about?

Figure 10 below indicates whether the controls that the banks implemented were effective in mitigating the risks that they were concerned about. The findings discussed in the preceding section indicate that only 75%(3/4) of the banks had security controls in place to address BYOD risks. Thus only three banks are considered in the analysis. Of these three banks, only two (66%) believed that the controls they implemented were effective in addressing the IT risks introduced by BYOD. This could be because these two organisations had done proper risk assessments prior to adopting BYOD, their responsibilities for managing BYOD were clearly defined and constantly updated according to latest threats and best practice regularly published by the Information Systems and Control Association (ISACA) and the International Standards Organisations (ISOs).

Figure 10: Analysis to determine whether controls implemented are effective
The remaining 33% (1/3) believed that the controls that it had currently implemented were not effective enough to address IT risks. The controls implemented at these organisations are still at maturity stage and organisations are facing BYOD threats on a daily basis. If not properly mitigated, IT risks can have an even greater impact on the business operations and objectives. However one can argue that an organisation can never be fully confident about the effectiveness of its controls as hackers are always coming up with innovative ways of accessing organisations’ infrastructure. Organisations are therefore constantly looking for new ways to control BYOD challenges as technology evolves.

4.4.10 Do you have controls in place to ensure that the privacy of employees’ personal information contained on the mobile device is maintained?

Figure 11 below indicates whether the sampled banks maintain the privacy of employees’ personal information. The results indicate that 75%(3/4) of the banks have controls in place to ensure employee privacy is maintained. These controls include ensuring that employees personal information is segregated from that of the organisation, strong authentication, encryption controls and wiping out the device in the event of it being lost or stolen. This is done to preserve the confidentiality of both the employee and the organisation’s information. However, 25%(1/4) of the sampled banks do not maintain the privacy of employees’ personal information.

Figure 11: Analysis of whether employees’ privacy is maintained

The importance of maintaining the privacy of employees’ personal information is addressed in section 2.8.1, which also highlights that this information should only be
obtained in a legal and fair manner to comply with regulatory requirements, especially when both business and personal information co-exists on the same device.

4.4.11 Are the bank’s infrastructure, mobile device operating systems and applications regularly updated to resolve security vulnerabilities and threats?

The results indicate that all the sampled banks understood the importance of updating their software and hardware with the latest security patches and took into account all devices (either personal device or owned by the organisation) when maintenance was done.

Maintaining an organisation’s infrastructure right from the database, operating system, application and network, is crucial for any organisation regardless of size, revenue or whether BYOD is adopted or not. To prevent unauthorised access and cyber-attacks, an organisation must ensure that its infrastructure is supported with the latest security software tools, patched against vulnerabilities and that cybereason is implemented. All the sampled banks were confident that their organisation’s infrastructure was up to date to respond to security vulnerabilities and threats and believed that the policy added benefit to the organisation.

4.5 CONCLUSION

The empirical research consisted of questionnaires that were completed by four representatives of the four biggest banks in South Africa. These participants were selected because of their extensive understanding of IT security controls and risks.

The findings above highlighted that the sampled banks had a common understanding of the IT risks that the organisation faced. These banks also implemented controls, such as a BYOD policy, to address IT risks and ensure that employees were aware of the risks introduced by BYOD. The banks also offered training when employees were on-boarded; this was conducted annually as part of compliance training. The training ensured that all employees were aware of current and emerging risks that could affect the organisation.

Seventy-five percent of the sampled banks also implemented effective controls to address the privacy of employees’ personal information. The importance and benefit of having
personal mobile devices was described and all the banks believed that mobile devices had benefited the banks and addressed some of the IT risks that BYOD presents.

Chapter Five presents the key findings from the literature review and empirical study. Chapter Five also provides an overview of how the research objectives were addressed.
CHAPTER FIVE: CONCLUSION

5.1 INTRODUCTION

The objective of this chapter is to summarise the findings of the literature review and the findings from the empirical research of this study. This chapter also highlights areas for future research.

5.2 DEDUCTIONS

5.2.1 Literature review

The literature review began by describing how the recent rapid advances in IT have reshaped the world, and particularly, the banking environment. IT is seen as the driving force that enables banks to make informed decisions regarding the products that they offer to the customers. Banks are constantly seeking new ways to stay innovative and competitive. BYOD is one of the measures that banks use to remain agile and provide services to their clients in a more efficient and effective way.

BYOD was defined as a trend whereby employees are allowed to use their personal mobile devices for work purposes. The characteristics of BYOD were also defined explicitly to explain BYOD in a broader sense. These characteristics include: mobility, mobile, mobile technology, consumerisation and computer-based. The benefits of BYOD were outlined as:

- Ease of access to information from any place at any time;
- Greater employee satisfaction because of the flexibility to work from any place at any time;
- Enhanced productivity as employees are not limited to eight hours of working from the workplace their hours can be extended as they are able to work from anywhere; and
- Reduced costs as employees pay for their mobile devices, office space is also reduced and less is spent on printed materials and stationery.

The literature review also acknowledged that with the benefits that BYOD introduces, there are also a number of challenges that organisations may encounter. The challenges
are twofold: threats and risks. The first aspect addresses the threats that mobile devices are exposed to, whilst the second aspect addresses the risks that the organisations are likely to suffer because of BYOD. Some of the threats that were described include: employees with malicious intentions to steal, delete or corrupt information assets, lost or stolen devices and malware. The latter was described as one of the biggest threats to the organisation and can take different forms: viruses, botnets, worms, rootkits, phishing and direct attack.

Key risks that might impact the organisations were described as operational risk, legal and regulatory risk, technology and data protection risks, infrastructure and device risks and lastly, financial risk. To mitigate these risks properly, it was explained that responsibility for BYOD security needs to be clearly defined. Both the employer and the employees were highlighted as the main role players in securing BYOD.

Risk assessment should be conducted by the organisation before deciding to adopt BYOD. This should include technical assessment to verify that any existing issues that have not been addressed are taken into account prior to implementing BYOD. Mitigation controls must also be adopted to ensure that the organisation does not suffer any losses as a result of BYOD.

Mobile device management and mobile device policies were described as one of the main mitigation controls that organisations can adopt. Mobile device management is critical in protecting mobile devices; it refers to the architecture of how the BYOD programme is designed and how the devices connect to the organisation’s network. It also involves security controls such as firewalls which can be set up to prevent cyber-attacks.

As part of managing the device, mobile device policies should also be implemented to manage the BYOD programme. Mobile device policies define how employees' personal devices should be on-boarded onto the organisation’s network. This includes: access controls, communication controls, classification of information, application controls and compliance controls. Other controls linked to risk management and safeguarding the integrity of the organisation’s information when it is contained on the employee’s personal devices were also addressed. These controls highlighted employee awareness and training and how information and the BYOD programme should be audited.

To assess whether the sampled organisations had implemented these controls, an empirical study was conducted where the four biggest financial institutions in the country
were assessed through questionnaires. The results of the questionnaires are summarised below.

5.2.1 Empirical study

The results of the empirical study are summarised below.

All four of the sampled banks understood BYOD and embraced the concept within their organisations. The participants were aware of IT risks that could arise as a result of BYOD, hence they have all implemented mobile device policies as one of the controls to address IT risks. Furthermore, all four banks updated these mobile device policies regularly or every two years to ensure that they were up to date with the latest security controls around mobile devices.

Although all four banks had a mobile device policy in place, only one bank allowed its employees to directly access the organisation’s network. Three of the sampled banks provided training and awareness to the employees to enable them to understand any IT risks and controls related to the protection of the organisation’s information assets when personal devices were on-boarded to the bank. Data leakage, malware, vulnerability and viruses were the common threats that the banks were faced with. Employees in all four banks were allowed to download external applications onto their personal mobile devices.

Not all of the banks believed that the controls they had implemented were effective. One of the banks had experienced an incident which the bank’s controls had not been able to prevent. Three of the sample banks also understood the importance of maintaining the privacy of employees’ personal information and implemented controls over the privacy of both the employees’ and the bank’s information.

All of the banks understood the importance of updating their software and hardware with the latest security patches and took into account all types of devices, whether mobile, desktop, laptop, when maintenance was done. All the banks believed that their mobile device policy had addressed the risks of BYOD for the organisation insofar as employees were more aware of the controls for BYOD and that the banks were able to keep track of any emerging risks and implement effective controls in time to address the risks.
5.3 AREAS OF FUTURE RESEARCH

Possible areas of future research are identified as:

- Evaluating IT risks stemming from the use of mobile devices for work purposes private and public companies and comparing the controls in public companies with those in private companies.
- Performing vulnerability and penetration assessments on employees’ personal mobile devices. This would be to evaluate whether the banks adequately assessed the security controls on these devices.

5.4 CONCLUSION

An empirical study was conducted on a sample of four South African banks. The results of the empirical study were analysed and indicated that all of the sampled banks were aware of the BYOD concept, its advantages and challenges. All banks affirmed the importance of having a mobile device policy as one of the controls to govern the security of mobile devices.

The above findings also indicate that all the banks provided training and awareness to their employees when employees’ devices were on-boarded to the banks. The training fostered awareness of IT threats and risks that the organisation could be exposed to. The banks further indicated that they allowed employees to download external applications onto their mobile devices because the banks have no control over employee’s devices and this did not pose a risk to the banks as employees were not allowed to directly access the organisation’s network. Furthermore, all the banks updated their mobile devices policies regularly to keep up to date with emerging risks.

The findings of this research indicate that when organisations decide to adopt BYOD, IT risks are introduced to the organisation. It is important for organisations to implement controls to address the risks and ensure that the controls are reviewed regularly to keep up to date with emerging risks that threatens the organisation.
REFERENCES


Harris, M. A., Patten, K. & Regan, E. (2013). The need for BYOD mobile device security awareness and training.


Safari, A. & Khalaf, A. (2013). *e-Commerce in Developing Countries: With Focus on e-Security (ECDC), 2013 7th International Conference on*. Conference proceedings of the Xth conference held in Y. IEEE.


Schalow, P. R. (2013). *ECIS*. Conference proceedings of the Xth conference held in Y.


Annexure 1

COVER LETTER – SURVEY QUESTIONNAIRE

An evaluation of information technology risks using personal mobile devices for work purposes

Dear potential research participant,

You are invited to participate in a research study that forms part of my formal MCom study.

Information is a vital asset of any organisation with tangible value that is core to a bank’s business. The increasing regulatory requirements with regard to Basel III, King IV and the increased focus on good corporate and IT governance makes it imperative that the banks take appropriate steps to ensure that information and information systems are properly protected from various threats. The organisation has the responsibility to keep information assets safe and secure. Information security policy and a set of procedures that define the security management standards is the first step in defining a framework to secure and pretend the bank’s information and information system.

This survey relates to making an assessment of how the banks relate to Information Technology (IT) security policies in addressing the risks that arises as a result of using personal mobile devices for work purposes. This study is being conducted by Ms. Tshimangadzo Brenda Sikhala (Sikhalab@gmail.com), as part of the completion of a dissertation to complete a Master’s degree in MCOM (Computer Auditing) at the University of Johannesburg during 2018. The title of the study is “An evaluation of Information Technology risks from using personal mobile devices for work purposes” and is being supervised by Mrs. Vanessa Van Dyk (vanessavd@uj.ac.za) and co-supervised by Ms. Pranisha Rama (pranishar@uj.ac.za)

IT risk within the banking industry as a result allowing employees to use their personal devices for work becomes more important in view of the ongoing financial and economic crises as a result of cyber-attack. The ability to safeguard information residing on mobile devices is a key component of information risk management within a bank. Having a mobile device policy will provide the banks with greater chances of avoiding incidents such as significant security breach, which could jeopardize the bank’s reputation.

The purpose of this study is to evaluate IT risks from allowing employees to bring their personal mobile devices, connect to the organisation’s network and use their device for work purposes as part of the daily operation. This ensures that the employees remain productive at all times while the organisation is meeting its objectives. However, it is important to also evaluate the negative effects it might have on the organisation.

Your willingness to voluntarily participate in this survey is greatly appreciated and contributes to the creation of new knowledge. You are hereby informed that your responses will be completely anonymous, which means that no personal details of your identity or the organisation you are employed by are submitted by you in this survey, which means that your responses can in no way be traced back to you personally as an individual or organisation. Results from all of the respondents will be collated and reported on as a unit, and your specific responses will not be reported on individually.
As a voluntary respondent, you are not obligated in any way to participate in this study and may choose to withdraw from the process at any stage without fear or consequence. Your right to privacy, confidentiality, and anonymity, equality, justice, and human dignity, freedom of choice, freedom of expression, access to information and access to the science community will be respected and not divulged to any third parties.

Please respond as openly and as frankly as possible to the questions.

Please acknowledge that you have read and understood the above information and that the data collector who is conducting this survey/interview with you has explained it adequately, by making a cross or a signature in the space provided below.

(Tick with X if relevant) I, as respondent, understand my rights in this process and proceed willingly and voluntarily with the survey.
Annexure 2

Questionnaire: To the Big Four Banking Organisations

Instructions:

1. This questionnaire can be completed manually.
2. Manual completion:
   - Please print and complete the questionnaire.
   - Please return the questionnaire by emailing the scanned document to: Sikhalab@gmail.com
3. Please do not hesitate to supply more information that might be relevant to this study.
4. The return date for the completed questionnaire is 23 March 2018.
5. Should you wish to contact Brenda Sikhala, she can be reached on 073 390 8286 or sikhalab@gmail.com.
1.1. Do you have a mobile device policy in place?
Yes ☐ No ☐

2.1 How are employees’ personal mobile devices on-boarded onto the organisation’s network?
………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………

3.1 Do you offer training to employees prior to on-boarding?
Yes ☐ No ☐
If yes, what kind of training is offered?
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………

3.2 How do you ensure all employees within the organisation are aware of the mobile device policy?
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………

4.1 What are the major IT risks that the organisation is exposed to when employees make use of their personal devices for work purposes?
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………………………

5.1 Do you allow employees to download any external applications on their personal devices?
Yes ☐ No ☐
6.1 Have you had any incidents of data breach as a result of employees using their personal devices for work?

Yes ☐ No ☐

If yes, please provide an example of such a data breach.

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

6.2 Do you believe that the controls that the organisation has implemented are effective to mitigate the risks the bank is concerned about?

Yes ☐ No ☐

6.3 Please describe some of the controls that the organisation implements to mitigate the risks that emanate from this and how do you control these risks?

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................

7.1 Do you have controls in place to ensure that the privacy of employees’ personal information contained on their mobile device is maintained?

Yes ☐ No ☐

If Yes, what are some of the controls have you implemented?

........................................................................................................................................................................
........................................................................................................................................................................
8.1 How often is the policy updated?

8.2 Are the bank’s infrastructure and mobile device operating systems and applications regularly updated to resolve security vulnerabilities and threats?

Yes ☐ No ☐

8.3 Do you believe the policy had added benefit in how the organisation manages risks?

Yes ☐ No ☐

If so, what kind of benefits has the bank derived?

Thank you for taking the time to complete the questionnaire. Please remember to scan and return to: Sikhalab@gmail.com