

Governing information security within the context of “Bring Your Own Device” in Small, Medium and Micro Enterprises

By

Noluvuyo Fani

2017

Governing information security within the context of “Bring Your Own Device” in Small, Medium and Micro Enterprises

By
Noluvuyo Fani

Submitted in fulfilment of the requirements for the degree
MAGISTER OF
INFORMATION TECHNOLOGY
in the
FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND
INFORMATION TECHNOLOGY
of the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Prof. Rossouw von Solms

Co-Supervisor: Prof. Mariana Gerber

2017

Declaration

I, Noluvuyo Fani, hereby declare that

- the work in this dissertation is my own work
- all sources used or referred to have been documented and recognised
- this dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.

Noluvuyo Fani

Abstract

Throughout history, information has been core to the communication, processing and storage of most tasks in the organisation, in this case in Small-Medium and Micro Enterprises (SMMEs). The implementation of these tasks relies on Information and Communication Technology (ICT). ICT is constantly evolving, and with each developed ICT, it becomes important that organisations adapt to the changing environment. Organisations need to adapt to the changing environment by incorporating innovative ICT that allows employees to perform their tasks with ease anywhere and anytime, whilst reducing the costs affiliated with the ICT.

In this modern, performing tasks with ease anywhere and anytime requires that the employee is mobile whilst using the ICT. As a result, a relatively new phenomenon called “Bring Your Own Device” (BYOD) is currently infiltrating most organisations, where personally-owned mobile devices are used to access organisational information that will be used to conduct the various tasks of the organisation. The use of BYOD in organisations breeds the previously mentioned benefits such as performing organisational tasks anywhere and anytime. However, with the benefits highlighted for BYOD, organisations should be aware that there are risks to the implementation of BYOD. Therefore, the implementation of BYOD deems that organisations should implement BYOD with proper management thereof.

Acknowledgements

- My two mentors and supervisors, Prof Rossouw von Solms and Prof Mariana Gerber, thank you, thank you, thank you for believing in me, for providing constant guidance supported by constructive feedback and the sharing your expertise/knowledge during this venture.
- My husband, Sando, for literally holding my hand, nurturing my heart with positive words of love and encouraging me as you maintained that I would complete this journey through faith, love and God.
- To my parents, Ncumisa Fani and Lindile Fani, thank you for understanding that this is a part of my journey and for the support/love.
- Lastly, to National Research Foundation (NRF) and the NMMU scholarship, thank you for the financial assistance towards this research.

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1. BACKGROUND	1
1.2. INFORMATION IN ORGANISATIONS	2
1.2.1. Information asset	2
1.2.2. Securing information	3
1.2.3. The Development of Information and Communication Technologies (ICT) and Mobile Devices	3
1.3. BRING YOUR OWN DEVICE	4
1.4. SCOPE AND DELINEATION.....	5
1.5. RESEARCH OBJECTIVES	6
1.6.2. Secondary research objectives.....	6
1.6. RESEARCH APPROACH.....	7
1.7. LAYOUT OF THE STUDY	7
1.8 CONCLUSION	8
CHAPTER 2: INFORMATION AS AN IMPORTANT ORGANISATIONAL ASSET.....	9
2.1. INTRODUCTION	9
2.2. WHAT IS INFORMATION?.....	9
2.3. WHAT IS INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)?.....	10
2.4. INFORMATION WITHIN AN ORGANISATION	12
2.4.1. Information as a business asset within organisations.....	12
2.4.2. The utilisation of information.....	13
2.5. INFORMATION SECURITY	15
2.5.1. Information security incidents and attacks:	15
2.5.2. Preservation of information	18
2.5.3. Information Security measures	19
2.6 CONCLUSION	20
CHAPTER 3: THE DEVELOPMENT OF COMMUNICATION TECHNOLOGIES	21
3.1 INTRODUCTION	21
3.2. THE HISTORY OF COMMUNICATION TECHNOLOGIES	21
3.3. MOBILE DEVICES.....	25
3.3.1. The history of telephones	25
3.3.2. The impact of wireless technology on mobile devices	26
3.3.3. The proliferation of mobile devices.....	28
3.4. BRING YOUR OWN DEVICE	29

3.4.1. What is BYOD?	29
3.4.2. Benefits of BYOD	30
3.4.3. Risks of BYOD.....	32
3.4.4. BYOD within organisations	33
3.5. SMMES.....	35
3.6. CHALLENGES OF SMMES.....	37
3.7. BYOD AND SMMES.....	40
3.8. CONCLUSION	41
CHAPTER 4: RESEARCH DESIGN.....	43
4.1. INTRODUCTION	43
4.2. RESEARCH PARADIGM.....	43
4.3. RESEARCH PROCESS.....	45
4.4. CONTEXTUALISED RESEARCH PROCESS	48
4.5. RESEARCH METHODS	52
4.6. CONCLUSION	54
CHAPTER 5: THE DEVELOPMENT OF THE BYOD MANAGEMENT FRAMEWORK.....	55
5.1. INTRODUCTION	55
5.2. PHASE 1: FRAMEWORKS FOR BYOD	56
5.3.1. Phase 2: Identified existing frameworks for BYOD.....	57
5.3.2. Evaluating the existing frameworks for BYOD.....	62
5.4. PHASE 2.2: CHARACTERISTICS AND PRINCIPLES OF THE BYOD MANAGEMENT FRAMEWORK	65
5.4.1. Principles of the BYOD Management Framework.....	65
5.4.2. Characteristics of BYOD	66
5.5. PHASE 2.3.: THE DEVELOPMENT OF THE BYOD MANAGEMENT FRAMEWORK	68
5.5.1. Initial BYOD Management Framework.....	68
5.6. PHASE 3: PROCESS TO THE REFINEMENT OF THE BYOD MANAGEMENT FRAMEWORK.....	72
5.6.1. Phase 3.1 - Phase 3.4: [Cycle 1] Data collection and analysis of the theoretical framework.....	73
5.6.2. Phase 3.5.: [Cycle 2] Refinement of the theoretical framework (mind map).....	74
5.6.3. Phase 3.5.: [Cycle 3] Refinement of the theoretical framework (focus group).....	75
5.6.4. Cycle 4: Refinement of the theoretical framework (questionnaire and semi-structured interviews)	76
5.7. BYOD MANAGEMENT FRAMEWORK.....	78
5.8. CONCLUSION	85
CHAPTER 6: VALIDATION OF THE BYOD MANAGEMENT FRAMEWORK:	86
6.1. INTRODUCTION	86
6.2. DATA COLLECTION.....	86

6.3. DATA ANALYSIS AND RESULTS	90
6.3.1. Results on the Principle of Scalability	90
6.3.2. Results on the Principle of Utility	91
6.3.3. Results on the Principle of Efficacy	93
6.3.4. Results on the Principle of Quality	94
6.4. FINDINGS	94
6.5. CONCLUSION	97
CHAPTER 7: CONCLUSION:.....	99
7.1. INTRODUCTION	99
7.2. SUMMARY OF FINDINGS	99
7.3. MEETING THE OBJECTIVES	101
7.4. SUMMARY OF CONTRIBUTIONS.....	102
7.4.1. Research Contribution: The artefact.....	102
7.4.2. Adherence to Research Paradigm Principles	104
7.4.3. Methodological Contribution	106
7.4.4. Academic Publications.....	107
7.5 FUTURE RESEARCH	107
7.6. EPILOGUE	108
REFERENCES	109

List of Figures:

<i>Figure 3.1: Challenges or barriers of BYOD</i>	33
<i>Figure 3.2: Five phases of SMME development</i>	36
<i>Figure 4.1: Four-phased approach for design-oriented IS research</i>	44
<i>Figure 4.2: Four-phased approach for design-based research</i>	45
<i>Figure 5.1: BYOD Security Framework (Zahadat et al., 2015)</i>	58
<i>Figure 5.2: BYOD framework for a management system (Brodin, 2015b)</i>	59
<i>Figure 5.3: BYOD privacy & culture governance framework (Selviandro et al., 2015)</i>	60
<i>Figure 5.4: Enterprise and BYOD space BYOD Security Framework (Wang et al., 2014)</i>	62
<i>Figure 5.5: Initial draft of the theoretical framework (Noluvuyo Fani)</i>	69
<i>Figure 5.6: The first aspects in the theoretical framework</i>	70

<i>Figure 5.7 : The third aspects in the theoretical framework</i>	70
<i>Figure 5.8: The theoretical framework for BYOD</i>	71
<i>Figure 5.9: Partial representation of the mind map</i>	75
<i>Figure 5.10: Refined theoretical framework</i>	76
<i>Figure 5.11: Sample questionnaire questions</i>	77
<i>Figure 5.12: The process model of the cycles of refinement</i>	78
<i>Figure 5.13: BYOD Management Framework</i>	79
<i>Figure 5.14: BYOD Security Requirements</i>	79
<i>Figure 5.15: BYOD Security Management</i>	80
<i>Figure 5.16: BYOD Management System</i>	81
<i>Figure 5.17: BYOD Strategy</i>	81
<i>Figure 5.18: BYOD Policy Plan</i>	83
<i>Figure 5.19: BYOD Policy Implementation</i>	83
<i>Figure 5.20: BYOD Compliance</i>	84
<i>Figure 6.1: Four phases of the research process</i>	86
<i>Figure 6.2: Extracted an example of the BYOD policy</i>	88
<i>Figure 6.3: Extracted an example of the validation questionnaire</i>	89
<i>Figure 6.4: Results on the Principle of Scalability</i>	91
<i>Figure 6.5: Results on the Principle of Utility</i>	92
<i>Figure 6.6: Second Set of Results on the principle utility</i>	92
<i>Figure 6.7: Results on the Principle of Efficacy</i>	93
<i>Figure 6.8: Results on the Principle of Quality</i>	94
<i>Figure 7.1: Final BYOD Management Framework</i>	103

<i>Table 1.1: List of Appendices and Explanations</i>	8
<i>Table 4.1: Research process (Herrington et al., 2005)</i>	46
<i>Table 4.2: Implementation of the research process</i>	48
<i>Table 4.3: Research methods</i>	52
<i>Table 5.1: Phase 1 of the research process</i>	56
<i>Table 5.2: Phase 2 of the research process</i>	57
<i>Table 5.3: Evaluation of the existing BYOD frameworks</i>	63

<i>Table 5.4: Phase 3 of the research process</i>	72
<i>Table 6.1: Workshop Questionnaire Structure</i>	89
<i>Table 6.2: Stakeholder feedback results combined</i>	95

Chapter 1: Introduction

1.1. Background

Employees are fundamental to the successful running of most organisations, more so the information they utilise in order to conduct their tasks. Information can be utilised to formulate a report for the management of finances in an organisation (Broadbent, 1998). In essence, information supports the achievement of organisational tasks. Subsequently, it can be deduced that, information is considered an asset within any well-run modern organisation.

With the foregoing in mind, it is important to understand that information is an intangible asset, as it can neither be seen nor touched. However, even though the information is intangible, there exists various threats that can attempt to infiltrate and expose its integrity or sensitivity. This is most likely the case when organisations do not properly manage the protection of information (Brody, Mulig & Kimball, 2007). In order to address various existing threats, organisations utilise various security mechanisms. These include software and hardware systems such as antivirus and password encryption systems (Caldwell, 2011). In using these security mechanisms, organisations establish some form of protection of information against threats. This, in turn, leads to employees being able to access, communicate, process, and store sensitive information within controlled boundaries.

In this modern day, employees access, communicate, process, and store information through advanced technologies, such as computers, mobile devices, and in other electronic gadgets. Accordingly, the requirements for employees, when conducting most organisational tasks, have been evolving. As a result, technology should constantly be developed in order to adhere to the changing requirements. An example of these requirements includes Information and Communication Technologies (ICT) that allow ease of use for employees, whilst reducing the costs affiliated to the management of the ICT. Consequently, ICT has since been developed to adapt to the requirements of organisations. This has been done with the innovative development of mobile devices, such as smartphones amongst others. These mobile devices allow access to information, such as emails, spreadsheet based information and other types of information (Andrew, 2012).

Most recently, a new technological phenomenon for mobile devices called, 'Bring Your Own Device' (BYOD) has been introduced. BYOD allows for ease of using an employee's personal mobile device to access, communicate, process and store organisational information within or outside the boundaries of an organisation. Moreover, the organisational expenses associated with the use of BYOD are reduced. This is due to the employee typically purchasing the personal mobile device (Weeger & Gewald, 2014).

Nonetheless, most organisations, both large and Small-Micro and Medium-sized Enterprises (SMMEs) are adopting BYOD. As with other ICT instances, there exists risks associated with BYOD (Self & Kestle, 2013). As a result, it is essential to consider the importance of information in an organisation and how they could protect their information. Furthermore, it is important to understand the development of ICT, BYOD, and the effect of BYOD in SMMEs.

1.2. Information in organisations

From the foregoing, it is clear that information is important as it is used to conduct most tasks in an organisation. This holds for modern organisations in general, which include SMMEs. Thus, it is important to understand the link between general information usage and typical SMMEs.

1.2.1. Information asset

Information is intangible and cannot be touched or measured. Nonetheless, information is used to run most tasks in SMMEs and other institutions alike. With regards to SMMEs, it can be stated that a typical SMME is a small business enterprise that provides services and jobs to the community (*National Small Business Amendment Act, 2004*). Although SMMEs are small in their nature, the information contained within their enterprises is considered a valuable asset. This is due to information being key to the running of most SMMEs and as a result it should be constantly protected (Moody & Walsh, 1999).

Unfortunately, SMMEs are facing challenges with the constant protection of information. This is most likely due to limited resources, amongst other causes. Accordingly, it may also be difficult to find the correct security mechanisms that SMMEs can use to protect their sensitive information. However, SMMEs could identify how they use their information, in order to gain a better understanding of how they could protect it (Coulson & Zhu, 2005). With

this in mind, an important aspect to consider is the securing of information within typical SMMEs.

1.2.2. Securing information

Information used within an organisation is communicated, processed and stored using various software, hardware, and other forms of ICT. The ICT utilised is susceptible to threats that could harm the quality of the information. Consequently, security mechanisms, like password encryption, are needed to authorise employees and protect the availability, confidentiality and integrity of the organisation's information (ISACA, 2010).

Furthermore, employees use the organisation's information to conduct most organisational tasks. Therefore, employees need to be aware of their role in protecting the information they use. In order to assist employees with awareness, organisations could implement education and awareness programmes to inform employees on their role in the protection of information (Redman, 2008).

Taking all the foregoing into consideration, it is clear that ICT has played a pivotal role in the use of information. Therefore, it is important to discuss how ICT assists organisations in conducting their everyday tasks.

1.2.3. The Development of Information and Communication Technologies (ICT) and Mobile Devices

During the 1960's, the communication of information took place through computers and telephone networks (Rao & Nayak, 2014). With time, the computers and telephone networks that were used advanced tremendously. As a result of the advancements, ubiquitous computing technologies emerged, such as laptops and mobile devices (Attaran, 2004). The mobile devices, permitted a user to communicate, process and store information whilst being mobile. Furthermore, the proliferation of mobile devices grew to incorporate the use of mobile devices within organisations (Widen-Wulff, 2004).

The infiltration of mobile devices in organisations warranted the use of mobile devices by numerous employees. Consequently, to adapt to the organisational environments, wireless communication was proliferated. It began with the generation of radio-frequency technology and grew into the current generally used Fourth Generation (4G) wireless technology. As a

result, 4G allowed wireless communication between various ICT systems, such as mobile devices (Pachauri & Singh, 2012).

As the years progressed, there were further developments in wireless technologies and mobile devices. In this modern day, mobile devices are used in most organisations as they provide the employees with the flexibility of using their personal mobile devices as an official device (Becher et al., 2011).

Subsequently, the integration of mobile devices into personal and official devices has resulted in the phenomenon of BYOD. Even though BYOD is a relatively new phenomenon, this does not hinder the increase of its adoption in most organisations.

1.3. Bring Your Own Device

Sheridan, Ballagas and Rohs, (2004), define BYOD as, “...*the circumstance, in which users make their own personal devices available for company use; and these user devices enter the workplace*”. However, BYOD is commonly associated with ICT consumerization which is defined as “*Private or personally owned ICT resources, such as computer hardware devices or software, that are used for business purposes*” (Niehaves, Köffer, & Ortbach, 2012). Nevertheless, BYOD is described by multiple definitions, although there is not one that is clear and distinct. For this reason, it is important to consider the benefits that BYOD provides. The various benefits that are gained by the organisations that implement BYOD include the following:

- **“Anything”:** This means that the employee’s personal mobile device can be used to communicate, process and store organisational tasks outside the boundaries of the organisation;
- **“Anywhere”:** Mobile devices can be used to connect to wireless networks and technologies that do not form part of the organisation
- **“Anytime”:** The employee can use their personal mobile device anytime, at home or in the organisational boundaries.

The benefits associated with BYOD mean that most organisations would want to adopt it. It is also a phenomenon that is not limited to the size of an organisation. As a result, both large organisations and more importantly, in this case, SMMEs could implement BYOD within the

organisation's infrastructures. Nonetheless, there exists various risks that are associated with BYOD and these include but are not limited to malware and phishing attacks. For this reason, it is likely that SMMEs will adopt BYOD with limited thought on the implementation of its programmes. Consequently, this could lead to serious adversities that the SMMEs might not be able to recover from.

From the onset, it is clear that with the advancement and growth of mobile technologies, enterprises in general which includes SMMEs in South Africa, feel the pressure to utilise and incorporate the BYOD phenomenon. Unfortunately, BYOD leads to incorporating the problems and risks associated with the utilisation thereof.

Therefore, the problem addressed in this study can be stated as follows:

BYOD is a phenomenon that can cause information related risks in SMMEs.

Supporting the stated problem, the thesis statement addressed in this study can be phrased as follows:

The information security related risks associated with BYOD in a typical SMME environment can be mitigated with the sound governance thereof.

With the identified problem and thesis statement in mind, it is important to consider exploring the scope, objectives and research approach of this study.

1.4. Scope and Delineation

BYOD is a phenomenon that is associated with various benefits and risks. However, organisations, like SMMEs are more susceptible to these risks. This is most likely due to the fact that SMMEs have limited security mechanisms to protect their information (Johnson, Twilley, Zhang, Zhou, & Wu, n.d.). This includes the lack of proper ICT departments that will be responsible for the organisation's software, hardware and other ICT related duties (Pinzon, 2008). Subsequently, the information in SMMEs becomes a target for attackers and therefore, effective management and control for BYOD should be implemented in SMMEs.

According to the National Small Business Amendment Act 29 (2004), an SMME is a relatively small business enterprise or a distinct entity which branches into smaller subsidiaries. SMMEs provide services, programmes and jobs that improve the economy(National Small Business Amendment Act, 2004). This will improve the economy of the community.

It is clear from the foregoing that SMMEs experience problems as far as technology development, limited budgets and expertise are concerned. These problems pose risks to the information contained within the BYOD devices, as most SMMEs are likely to adopt the phenomenon with a lack of proper management. Therefore, it is clear that BYOD is a problem situation experienced in SMMEs and it needs to be governed properly (Ghosh & Rai, 2013).

Taking into consideration the foregoing, it is important to consider the objectives of this study.

1.5. Research Objectives

The primary objective of this study is:

To formulate a framework towards governing information related risks associated with the rollout of BYOD in a SMME environment.

The secondary research objectives are as follows:

- 1. To study the information related risks associated with BYOD in a typical SMME environment.*
- 2. To identify governance related sources currently in place for BYOD that could be utilised in a SMME environment.*
- 3. To formulate a governance-orientated contribution towards mitigating information related risks of BYOD in a SMME environment.*

This study aims to address a real-life problem that exists within SMMEs. Therefore, the above-mentioned secondary objectives aim to collectively address this real-life problem.

Nonetheless, to achieve the primary objective of this study, a suitable research approach must be devised.

1.6. Research Approach

The implementation and utilisation of the BYOD phenomenon is associated with a real-life problem. To address this problem, this study will compose an artefact. This artefact will be in the form of a framework towards governing information related risks associated with the rollout of BYOD in an SMME environment. Therefore, design-oriented Information Systems (IS) research was selected as the logical research paradigm. An extensive and detailed discussion on design-oriented IS research, the research process and methods followed will be espoused in Chapter 4.

1.7. Layout of the Study

This chapter consists of a discussion on the background of the study. Furthermore, the problem area, primary and secondary research objectives and the research design aimed to address the real-life problem at hand will be highlighted. With the objectives of this study clearly defined, Chapter 2, will commence by addressing the role of information in organisations.

ICT facilitates an environment in which organisations can use information. Chapter 3 highlights the history of ICT and the way ICT influenced organisations. Furthermore, Chapter 3 discusses the concept of SMMEs and the adoption of BYOD in these SMMEs. As a result of this, a real-life problem has been identified, that of the adoption of BYOD within SMMEs. Thus, Chapter 4 provides the research approach used in this study to addresses the problem at hand.

With the research approach stipulated, Chapter 5 highlights the development of the artefact in the form of a framework, which is the primary research contribution. This framework is termed the BYOD Management Framework. Upon the completion of the development of the BYOD Management Framework, Chapter 6 will provide details on the validation process for the BYOD Management Framework. The final chapter, Chapter 7 will conclude this study by providing a summary of the research findings of this study.

Additionally, in order to support the research conducted, various supporting appendices are included in this study. The appendices include two papers that were presented at conferences, as espoused in **Error! Reference source not found.:**

Table 1.1: List of Appendices and Explanations

Appendix A	An illustration of the mind map formulated in this research
Appendix B	A questionnaire was used to determine the requirements for BYOD in the SMMEs.
Appendix C	A questionnaire was used to validate the solution.
Appendix D	A draft of the BYOD policy.
Appendix E	Research paper: Governing information security within the context of “Bring Your Own Device in SMMEs”.
Appendix F	Research paper: A framework towards governing “Bring Your Own Device in SMMEs”.

1.8 Conclusion

A background of this study was provided in this chapter. In the discussion of the background, the importance of organisational information was emphasised. In this modern day, organisational information is made available through mobile devices, consequently, the phenomenon of BYOD was briefly detailed. The discussion of BYOD revealed that various organisations, particularly SMMEs, are adopting this phenomenon in their respective organisations because of its benefits which includes the access to organisational information anywhere. However, there is the real-life problem of risks associated with BYOD. As a result, this chapter discussed the problem identified for this study. Thereafter, a discussion on the objectives and research approach that would be used to address the problem concluded the chapter.

With this in mind, it is important that the chapter that follows discusses the importance of information in organisations.

Chapter 2: Information as an important organisational asset

2.1. Introduction

Within any organisation, employees conduct and complete various daily tasks as part of their job function. Information facilitates the process of conducting and completing these daily tasks. Furthermore, the information will be utilised by the employees when they make decisions on certain issues (Zafar, 2013). In most instances, the tasks include the processing, communication and storage of information. When information is processed, communicated and stored, it generally uses ICT (Lindsay, Downs, & Lunn, 2003).

The way each organisation utilises information will be distinct, as each organisation will make decisions, process, communicate and store information according to their tailored specifications. As a result, the distinct way that each organisation utilises its information, will provide them with a competitive edge (Crees & Self, 2013).

Thus, information plays a pivotal role in conducting different tasks within the organisation, which makes it a valuable asset. With information being of value, there should be measures put in place to protect this information and therefore, information protection should be at the forefront of each organisation (Fakhrutdinova, Kolesnikova, Yurieva, & Kamasheva, 2013).

Information security assists organisations in the process of protecting its information. When implementing information security to the organisational information, ICT and other mechanisms should try to ensure that the information remains confidential, the integrity of the information remains intact and the information is constantly available in order to complete the daily business tasks (Brody, Mulig, & Kimball, 2007).

Thus, this chapter aims to provide an understanding of information in an organisational context and the importance thereof. Therefore, this chapter will discuss what information is and its importance. Thereafter, there is a discussion on the role of ICT and the utilisation of information within an organisation. Finally, this chapter ends with a discussion on the way information security assists in protecting information from incidents and attacks.

2.2. What is information?

Information is commonly associated with data. However, data and information have two different meanings. Data is raw, unprocessed, unorganised attributes or computerised facts

and numerical data. It can be represented as symbols, characters, graphs or figures (Monreale, Rinzivillo, Pratesi, Giannotti, & Pedreschi, 2014) (Monreale et al., 2014). However, the data is raw, unprocessed, unorganised computerised facts and numerical data, it will need to be analysed and processed before it can be used. When the data is analysed and processed, it can be referred to as information (Redman, 2008).

Information can thus be seen as analysed and processed data. There are different formats for information and these include documents, audio and visual formats (El-Tawy & Abdel-Kader, 2012). Information can be partitioned into different types of categories. The types of categories for information are inclusive but not limited to personal information and intellectual information (ISO 27002, 2013).

Information is gathered to determine which part of it is relevant in supporting the work-related organisational tasks. For example, the information gathered will be inclusive of information about current/potential clients, the organisations employees or the organisations intellectual property (Pesrsonneault & Kraemer, 2014). Once the relevant information is gathered, it can be captured, processed, communicated and stored. The information gathering, capturing, processing, communication and storage is facilitated by ICT (Valdez-juárez, Lema, & Maldonado-guzmán, 2016).

2.3. What is Information and Communication Technology (ICT)?

The influence of information in daily life cannot be overlooked. For humans, information affects the decisions we make, whether one is at work, at home or at the grocery store. The information that is used by humans is normally communicated, processed or stored in some form of ICT. ICT is adopted into both personal and work life to be used to make the important decisions. The use of ICT allows individuals to access, process, communicate and store information anywhere and anytime. However, the relevance of the information will be determined by the specified environment (Koltay, 2011).

With the different environments and ways in which information/data with the assistance of ICT can be used daily, it is necessary to consider how information is formed. Borek, Kumar Parlikad, Webb & Woodall (2013), provide different stages of the information development lifecycle. The stages of the information development lifecycle are as follows:

Capture/Creation: In the initial stages of the lifecycle, the information/data will need to be created /captured before it can be used and this is facilitated by the use of ICT.

Organisation: Once the information/data is captured/created, it will be required that it gets organised in a meaningful way so that it can be accessed with ease.

Storage: Storage areas will need to be identified in order to store the captured/created information/data. Information/data will be stored on storage media such as hard drives, servers and other forms of ICT hardware and software.

Processing: When the information is stored, the information can be processed in order to be utilised within the organisation.

Distribution: As information is required, it should be possible to distribute it within the organisation where it will be used.

Usage: The distributed information is utilised to complete various business tasks within the organisation.

Archiving: Information within the organisation is archived when it is not used on a daily basis and stored so that it can be used in extraordinary circumstances.

Disposal: The final stage of the lifecycle of information is when there is a lack of value on information, so it is deleted and disposed of (Borek et al. 2013).

A real-life example of an environment where the different stages of the information development lifecycle is evident, is in an educational institution. In an educational institution, students apply for admission to a university. When the student applies, the information officer captures the relevant information about the student with the use of ICT. The information officer will then organise the information in the right format. Thereafter, the application administrator stores the information in the university database.

The applicant's matric symbols will be processed to determine whether the student qualifies to be accepted into the university. The applicant's results will be distributed to the Head of Department (HOD) for a final decision. The HOD will use the relevant information to make the final decision on admission. After the student graduates, the student's relevant information will be archived as it might not be used in the near future. After a specified period after the

student's graduation, the stored information is no longer relevant within the university and will be disposed of (Garba, Armarego, & Murray, 2015).

Information can be utilised to conduct various organisational tasks. However, how the information is utilised depends on the task being performed. The tasks that are performed are inclusive of gathering, capturing, communicating or storage of information.

From the above example, it is clear how ICT plays a role in the different stages of the information development lifecycle within the organisation. Therefore, it is evident that ICT is core and thus an important asset to an organisation along with the information.

The following section will discuss the utilisation of information to conduct the daily organisational tasks such as the communication, processing, storage and decision-making amongst employees.

2.4. Information within an organisation

Information is core to the facilitation of organisational tasks, business processes, communication and decision-making (Macgregor & Macgregor, 2006). Therefore, information is an important asset within organisations.

With this in mind, the business asset of information and the utilisation of information will be discussed within this section.

2.4.1. Information as a business asset within organisations

In this modern day, every organisation uses information. The use of information in any organisation depends on the quality of the captured information. Poor information hinders the growth of the organisation, as information contains valuable facts and details about specific business activities (Khan, Butt, Zaman, & Asger, 2013). Moreover, the employees will consistently communicate and share information with each other. Furthermore, the employees will use the information that is communicated and shared, in order to make informed decisions about every day duties and tasks. Therefore, organisations should fully embed and embrace information, as it will form the foundation of most tasks in the organisation (Moberly, 2014). The way that employees utilise the information to make the decisions, distinguishes each organisation from its competitors, as they all use information to their discretion. Thus, information is the lifeblood of most organisations (Self & Kestle, 2013).

Earlier in section 2.3, the information development lifecycle narrated an educational institution as an example of an environment that uses the different stages within the information development lifecycle. It was emphasised that organisations rely on information in order to make important decisions. Within the educational institution, the HOD made use of information that was processed, communicated and stored in order to make the important decision of accepting a student into the university (Garba, Armarego, Murray, & Kenworthy, 2015).

The example above affirms that information is important within an organisation. The information will be used by individuals such as managers in order to make decisions on important issues (Attaran, 2004). From the above subsection, it is evident that two role players are important in the utilisation of organisational information. Firstly, technology is utilised to capture, store, and process, communicate and store information. Secondly, employees utilise this information to perform daily tasks within the organisation. In doing so, employees continuously interact with technology. Therefore, the next subsections will discuss the role of employees and technology in the utilisation of information.

2.4.2. The utilisation of information

When employees want to utilise information for their daily tasks, they will continuously interact with technology to process, store and communicate information. Therefore, a brief discussion on each of the role players, namely employees and technology will follow.

Employees

Employees are core to the everyday functioning of the organisation. Whether an organisation is small or large, employees are required. They are required within the so that they can process and conduct daily tasks. Consequently, the processing of the daily tasks requires that the employees have access to information (Widen-Wulff, 2004).

The employee is able to access the information through ubiquitous technological systems, such as computers, smartphones and laptops (Niehaves, Köffer & Ortbach, 2012). Ubiquitous technological systems are constantly expanding and developing. The expansion and development of these systems has allowed employees to not only gain access to organisational information within the boundaries of the organisational infrastructure but also

from home, in another country and other destinations. This entails that the information could be accessed anywhere, anytime (Keyes, 2013). Consequently, when employees gain access to organisational information anywhere and anytime through the ubiquitous technological systems, there should be adequate security measures introduced.

Technology

An organisation is dependent on the technology (ICT) it utilises in order to achieve the success of completing day-to-day tasks (Bhat, Dalal, Deutsch, Goulías, Hu, Lei, Pendyala, Ravulaparthi & Yoon, 2010). As the organisation develops, the technologies required escalate as there are more employees and communication, storage and other organizational tasks need to be implemented in a timely manner using ICT. As the use of technologies increases, it is used in different means to implement the organisational business processes. This proposes the use of ubiquitous technologies such as laptops, smartphones and external hard drives. Thus, when the ubiquitous technologies are identified, they can be commissioned and dispersed among multitudes of various departments and staff employed within the organisation (Monreale et al., 2014). Once dispersed, they will be utilised for the communication, access to and processing of information with ease.

These technologies allow the access, processing and communication of large volumes of information. Thus, this allows organisations to complete their tasks with ease of use (Okello-Obura & Matovu, 2011). However, when there is technology used, organisations should incorporate security measures to protect not only the technologies but also the organisational information.

Therefore, the utilisation of information by employees and technology for different purposes provides evidence that information is an important business asset. This was evident in this section as it initially discussed the importance of information as a business asset. Employees and technology utilise information to conduct various daily tasks. Consequently, the role of employees and technology in the utilisation of information was also deliberated. Information and the related ICT resources are critically important within the organisation and therefore require protection.

2.5. Information security

Information is an important asset within the organisation. Various risks constantly threaten to compromise or expose organisational information. For this reason, it is important that there is constant protection to the information. This section will discuss information security incidents and attacks as well as the role of information security in the protection of information from these incidents and attacks.

2.5.1. Information security incidents and attacks:

The PricewaterhouseCoopers (PwC) 2016 Global State of Information Security Survey noted that, theft of “hard” intellectual property increased by 56% in the year 2015, additionally the reported incidents pertaining to information security, increased to 42.8 million. This indicates that there are 117,339 attacks each day. Furthermore, there is an indication that more cybercriminals are infiltrating South Africa as opposed to Europe. This is due to the success of law enforcement in Europe (PwC, 2016).

The 2013 Norton Report adds to the findings of the PwC report, as it reveals that South Africa ranks as a country with the highest number of cyber-crime victims, with 73% victims affected. The report states that 63% of those victims are mobile device owners. Furthermore, half of mobile device owners do not have a password or any security software to protect their devices from cyber-crime (“2013 Norton Report,” 2013).

The above reports justify that there are information security incidents and attacks plaguing organisations through ICT, specifically mobile devices. As a result, within this subsection phishing and malware are two prominent information security incidents and attacks identified that affect the mobile devices utilised by employees. Phishing and malware lead to cyber-crime, thus (Aakanksha, Ankit, Jain, & Agrawal, 2016). Therefore, there is a discussion of each in brief below.

Phishing

According to the RSA Online Fraud Resource Centre, mobile devices are one of four technologies susceptible to phishing attacks and in the year 2014, \$4.5 billion dollars was lost due to phishing attacks (“RSA Online Fraud Resource Centre,” 2014). From the findings, it is clear that a lack of information security within organisations does give rise to incidents and

threats that could infiltrate and harm the organisational information. Employees constantly access the organisational information through ICT. The organisational network is normally the access point for information security attacks and incidents (Wang, Wei, & Vangury, 2014). The aim of phishing is to manipulate the user within the organisation to reveal confidential information that will be utilised for financial gain by the attacker (Aakanksha et al., 2016).

According to Ollmann (2007), the term “phishing” originates from internet hackers who made use of email spams to “phish” for the users’ passwords and to “phish” for financial material. Within the word “phish”, “ph” is associated with hacking schemes such as “phreaks”, which are the original hackers who hacked telephone systems (Ollmann, 2007). A phishing attack is composed of the following steps (Chaudhry, Chaudhry, & Rittenhouse, 2016):

Lure: A phisher lures a user by sending an invite through a Short Messaging Service (SMS), an email or a link to a spoofed website that will look legitimate and lure the user to respond.

Hook: The user responds to the invite by viewing the SMS, email or link to a spoofed website and provides additional information requested. As the user has responded, or showed interest, they are therefore hooked.

Catch: The phisher has caught the user as they have received the information they required.

Once the individual or organisation is lured, hooked and caught, the perpetrator will gain access to the organisations valuable information. For example, the perpetrator can in some instances damage the reputation of the organisation by utilizing the information in malicious acts or through leaking the information. In other instances, the perpetrator will use the information for their own personal gain, such as stealing money (Self & Kestle, 2013).

The incidents and way in which the phishing attacks have developed and adapted to penetrate and gain access to the organisations information (Aakanksha et al., 2016). Therefore, any organisation should be aware of phishing as an incident or attack that could infiltrate and harm its information.

Malware

Mobile devices are prone to malware attacks because of the variety of applications, software and services associated with mobile devices. According to the Hewlett Packard Enterprise

(HPE) Security Research Cyber Risk Report 2016, there is a 153% annual increase of on mobile device malware. Android devices, in particular, are susceptible to mobile malware, because of third party applications installed on the devices. The malware embedded in most of the third party applications can gain access to the user's personal messages. This is inclusive of emails and SMS messages ("HPE Security Research Cyber Risk Report," 2016). If there is a lack of security within the mobile device, organisational information accessed, communicated, processed and stored within the device will be attacked and stolen (Ramu, 2012).

Malware refers to the applications that contain malicious data. These malicious applications penetrate the ICT, information and other applications (Ojalere, Abdullah, Mahmud, & Abdullah, 2015). The malicious applications typically consist of code, script or software that will alter its behaviour to appear non-malicious. This allows the malware to hide its existence from detection software's in organisations. Thus, both large and small organisations find it difficult to detect and protect their organisations from malware.

Attackers often utilise the most common form of communication to a user by sending them an email or a spoofed link, which a user can click. Once the victim opens the email or clicks on the spoofed link, the malware "infects" the specified system, network and information (Shahzad, Hussain, Naeem, & Khan, 2013). AV-TEST statistics report 390,000 new malicious programs are identified daily. Moreover, within the month of August 2016, there were approximately 500,000,000 new malware incidents identified in various institutions ("AV-TEST Malware Statistics," 2016).

From the increasing number of malware incidents and attacks, it becomes apparent that risks to the privacy and confidentiality of the organisational information can be disastrous to the image of the organisation. It is therefore important to constantly monitor and protect information (Selviandro, Wisudiawan, Puspitasari, & Adrian, 2015). Furthermore, it should be noted that the threats associated with phishing and malware lead onto cyber-crime.

Cyber-crime

Normally, phishing and malware lead on to cyber-crime, as attackers utilise ICT resources when they want to conduct illegal cyber-crime activities online. The illegal activities include but are not limited to gaining access to organisational information and exposing the

information. Cyber-crimes are becoming more refined as the development of technology permits the emergence of new and adaptable cyber-threats (Self & Kestle, 2013).

The Global Risks Report stated that 35% of the global population conduct their activities online on mobile devices. Furthermore, the report predicted that by the year 2020, 5 billion users would use mobile devices for online activities. Some of the users using the mobile devices consist of employees. However, the report indicated that most cyber-crimes within organisations go unreported, as victims prefer not to disclose that there was an attack on their ICT. Therefore, there should be security measures put in place within organisations to protect against cyber-crime (World Economic Forum., 2012).

Cyber security is a process that is used to protect organisational information from threats such as phishing, malware and cyber-crime infiltrating organisations. There are various technologies for securing organisational information from threats (Selviandro, Wisudiawan, Puspitasari & Adrian, 2015). The technologies consist of; antivirus software for scanning and removing unwanted emails, viruses and other malicious activities, cryptography or the encryption of data so that attackers are not able to analyse the data received, mobile security applications and software for securing mobile devices to name a few (Eslahi Meisam & Var Naseri Maryam, 2014). Therefore, with the security measures in place for cyber-crime, it is possible that organisations can protect their information from cybercriminals.

These incidents and attacks threaten to compromise the information of the organisation. Thus, organisations should protect their information through the preservation of Confidentiality, Integrity and Availability (CIA).

2.5.2. Preservation of information

Information security strives to preserve CIA of information. The components of CIA are as follows:

Confidentiality

Confidentiality is the act of trying to protect sensitive organisational information and ICT from any unauthorised access. When the information and ICT of the organisation are properly protected, the information will remain confidential (Mir, Dar & Quadri, 2011).

Integrity

The integrity of the information is dependent on the information remaining intact from any unauthorised changes. When information is being processed, communicated and stored, it should be trustworthy and accurate (Whitman & Mattord, 2011).

Availability

Information within the organisation is constantly processed, communicated and stored, thus, it should be available to the employees of the organisation at all times (Bhat et al., 2010).

The goal of each organisation should be to preserve the CIA of information through security measures (Garba, Armarego, Murray, et al., 2015). Usually, the security measures are defined and specified in documentation typically policies. This is inclusive of policies like the information security policy and the policy should be distributed amongst employees as they need to be informed about their responsibility in preserving the CIA of information in the organisation (Allam, Flowerday, & Flowerday, 2014). All employees ranging from a clerk or a CIO are required to comply with the policies specified by the relevant organisation (Zafar, 2013). Failure to comply with these policies will result in action taken against the employee (Merad, Dechy, Serir, Grabisch, & Marcel, 2013).

2.5.3. Information Security measures

Information security plays a pivotal role in the protection of information. According to Whitman and Mattord (2011), the following can be deemed as a definition for information security; to protect the CIA of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training, awareness, and technology (Whitman & Mattord, 2011).

Within organisations, there is communication media, technology and other content utilised on a day-to-day basis to facilitate employees to access and complete the various organisational tasks. Networks have permitted different technologies to process, transmit or store information. Due to the value imposed on the organisational information, the network is susceptible to incidents of malicious attacks (Swanson & Guttman, 1996). Perpetrators could attempt to infringe on the organisational information through incidents and malicious attacks, such as hacking. Therefore, it is important to protect all organisational information and technologies (Chen & Zhao, 2012).

It can be difficult for organisations to know how to implement security measures for protecting the valuable information from threats and attacks. For this reason, there are best practices, standards and guidelines that provide guidance on the implementation of information security in organisations (Susanto, Almunawar, & Tuan, 2011). ISO 27002 provides a set of control guidelines for how an organisation can protect their information from threats and attacks, with the implementation of information security standards and information security management practices(ISO 27002, 2013).

Organisations should constantly attempt to preserve or protect their information. However, before an organisation can secure, protect and manage their information, the incidents and attacks that threaten the information need to be identified and managed. Therefore, this section identified and discussed the information security incidents and attacks namely phishing, malware and cyber-crime, currently plaguing organisations and their ICT. Furthermore, this section discussed the role of information security in protecting the organisational information from the incidents and attacks.

2.6 Conclusion

Within this chapter, information is advocated as a valuable asset within organisations. Moreover, organisations utilise information for decision-making, communication, and the processing within day-to-day tasks, with the use of technologies. With the organisational information utilised on a day-to-day basis, with the use of technologies, this chapter highlighted that there is a need for the protection of information.

The value of information and related ICT resources was emphasised, along with the information security incidents and attacks that threaten these assets. Thereafter, a discussion on how organisations could protect their information from the incidents and attacks with the assistance of information security concluded the chapter.

The next chapter discusses how information is communicated using communication technologies. Within the chapter, the history of communication technologies and the role of the technologies utilised for communication are highlighted. Thereafter, there is a discussion on mobile devices and the phenomenon of BYOD.

Chapter 3: The development of communication technologies

3.1 Introduction

Communication is the process of exchanging thoughts, ideas or information through conversations, signals or behaviour. Communication promotes personal relationships, work-related partnerships and organisational tasks (Xu, 2016). The process of communication always involves a minimum of two parties, a sender and a receiver. The sender sends information to the receiver and only once the receiver understands the information, the communication can be deemed successful (Leonardi, Huysman, & Steinfield, 2013).

There are different channels utilised for conducting communication. During the last decades, ICT has been the main channel that assists in the implementation and management of communication. As a result, in this day, the way in which communication is conducted has developed to be largely dependent on ICT (Crowley & Heyer, 2015).

Thus, the aim of this chapter is to discuss the role of communication technologies when used for communication. The first section of the chapter discusses the history of communication technologies. Communication technologies are inclusive but not limited to mobile devices. A mobile device is a communication technology regularly utilised for communicating information in this modern day, therefore this chapter will also examine the context of mobile devices. Lastly, the proliferation of using mobile devices for communication has resulted in the development of the BYOD phenomenon. The phenomenon of BYOD is currently infiltrating organisations as employee-owned mobile devices become incorporated within organisations. Therefore, a discussion of BYOD will close this chapter.

3.2. The history of communication technologies

There are different ways to conduct communication; this can be through system-to-system interaction or perhaps between human to system or device interaction. Thus, with the different ways of communication, it is imperative to understand the overall history of communication technologies. Therefore, this section will detail an overview of the history of communication technologies that have supported communication over time.

Besides speech, handwritten text was one of the first basic forms of communication (Littlejohn & Foss, 2010). Text written by the hand can be time-consuming, thus with time,

communication technologies utilizing printed text, became popular. Although the handwritten text is being replaced by communication technologies such as printed text, there are circumstances such as filling in a document that still require the use of handwritten text (Poyatos, 2008).

In the year 1833, the telegraph was developed which was the first working communication technology that permitted printed text. It used electronic signals, which were transmitted through multiple wires to communicate and record telegraphic (brief) information or messages such as numerical values or alphabetic letters. The telegraph was widely used for conducting communication across the globe, however, as new technologies emerged, the telegraph was replaced by other technologies such as telephones and fax machines (Winston, 1998).

In the year 1876, Alexander Graham Bell invented the telephone. The purpose of the telephone was to communicate numerous verbal messages between two or more individuals. The telephone consisted of a generator with different apparatus that allowed an individual to communicate their verbal message to a receiver. The receiver of the verbal message would receive the message through a receiver tube. The message communicated between the sender and the receiver would be transmitted electronically through a wire. Telephones were common in most households, but smartphones and other types of mobile devices have through time, replaced the traditional telephones. However, telephones are still common in organisations as a necessary technology for communication (Crowley & Heyer, 2015).

With communication technology moving away from technologies such as telephones, IBM developed the mainframe computer, System/360, which was the first computer that was used in organisations to process large quantities of data (Shaikh & Karjaluo, 2015). It could conduct and store multiple operations because it had a 64-bit memory, which was a large storage capacity at that time. Although the mainframe computer had limited, if any, communication functionality, the development of the mainframe computer seized the opportunity of commercialising the technologies (Wilbanks, 1996).

Succeeding the mainframe computer were other revolutionary developments of communication technologies namely televisions. The communication technologies were successful in permitting the communication of information, however, they were lacking in

their inclusion of society. Furthermore, the invented communication technologies used in organisations, such as the mainframe computer, were expensive and too large to be utilised by multiple users at the same time (Metropolis, Howlett, & Rota, 2014).

As a result, it became evident that there is a need for a technology that is cost effective, small in nature and permits multiple users within society and organisations, to communicate and conduct different processes. This was more evident within the different departments of organisations, as there was a variety of information communicated, stored and processed by multiple employees (Attaran, 2004). Additionally, individuals wanted to be able to communicate and conduct personal and organisational tasks at home with the assistance of communication technologies (Vishwanath, 2016). Thus, the invention of minicomputers was evident.

After numerous versions and attempts, the first successful minicomputer to meet the specified needs of society and organisations weighed approximately 23 kilogrammes and could be moved and stored in storage areas such as cupboards. An individual using the minicomputer could communicate and conduct activities such as data processing, time-sharing of multiple operations at the same time, with network and telecommunication processes (Baecker & Kaufmann, 2014).

However, in order to conduct some of these activities, an individual had to use an external peripheral device. The external peripheral devices consisted of cassette tapes, cartridge discs and line printers to name a few. The user of the minicomputer would use a peripheral device, namely a keyboard, to input textual information and a monitor connected to the minicomputer would display the input text. Both the keyboard and monitor, would be linked to a Central Processing Unit (CPU), which would convert the input text to output readable text (Gessner, Girao, Karame, & Li, 2013).

The development of the minicomputers assisted users in the 1960s and 1970s, to communicate, store and process various personal or organisational input to produce output whilst reducing costs and storage capacity. Another invention that developed to communicate, store and process various input data to produce output data during the 1970s, was the Personal Computer (PC). The earliest version of the PC, referred to as Altair, had limited functionality

as it permitted users to input data with no peripheral device and would output flashing lights (Metropolis et al., 2014).

However, amendments and developments were made to the PC, and soon the functionality and its use infiltrated personal and organisational environments. Individuals utilised the PC with the use of peripheral devices such as a mouse or keyboard, to share files, input and print data, view and edit graphics, send and receive emails, play games and other functions (Myers, 1996). As the development of computers continued, there was the increased use of computers by multiple users, thus there was the need for faster connections and communication. Consequently, there was the development of the World Wide Web (WWW) and Local Area Networks (LANs).

The WWW and LANs assist users in accessing and using different websites and applications on the internet to promote communication. A LAN consists of cables, routers and other components that permit a network of computers and other communication technologies, connected together, to communicate information to each other. LAN typically permits short distance communication, thus, it will operate in a small infrastructure such as a group of buildings or an office. If a user wants to expand the network of communication, they can utilise Wide Area Network (WAN) instead of LAN. WAN spans over a large geographical distance of over one kilometre (Whitman & Mattord, 2011).

The invention of the different types of communication technologies discussed in this subsection revolutionized the history of ICT as it paved a way for the development of portable technologies (Tatnall, n.d.). One of the first known portable communication technology, that was a very small version of a PC, was a laptop. A laptop is composed of an integrated keyboard and monitor, a peripheral mouse and charger. The advantage of using the laptop is that it is portable. As a result, an individual could travel anywhere with the laptop (Harris & Patten, 2014).

The portable communication technologies have since advanced into the technologies known as mobile devices, which are inclusive but not limited to notebooks and smartphones. Mobile devices are becoming predominately used within the organisations and for personal and organisational tasks. Mobile devices permit verbal and written text communication on a single device. (Gandotra & Kumar, 2016).

As communication technologies developed and computing devices utilising these communication technologies got smaller, there was a huge shift towards individuals wanting to own their own personal devices to enable them to continuously communicate and stay connected to the internet. With this in mind, the context of mobile devices is discussed further in the section.

3.3. Mobile Devices

Prior to the 21st century, individuals such as employees used communication technology such as a telephone to communicate information. The communication technology would be connected to physical wire cables, fixed on a wall, which would make it difficult to be mobile whilst using the technology (Myers, 1996). However, with the developments of the communication technologies in history, being mobile and able to carry a device is the phenomenon of the 21st century. For that reason, mobile devices are widely utilised in the present day as portable communication devices or technologies (Baecker & Kaufmann, 2014).

A mobile device is a hand-held device that allows a user to be mobile while using the device. The mobile devices are inclusive of tablets, laptops and smartphones. Mobile devices offer the comfort and advantage of communication “wherever” or “whenever” (Lebek, Degirmenci, & Breitner, 2013). However, there are also risks or disadvantages associated with the use of mobile devices.

The following subsections will discuss the history of telephones, the impact of wireless technology on mobile devices and the influence that the mobile devices have on society and organisations.

3.3.1. The history of telephones

The origins of mobile devices stem from the telephone invented by Alexander Graham Bell in 1876. The telephone was composed of three box components:

Upper box section: A bell, crank and a magneto generator used to start the call on the box

Middle box section: An extended speaker tube for relaying a message and a receiver tube used to receive a message

Bottom box section: The bottom box had a cell battery connected to a wire. The cell battery would transmit the communication of the message

The development of the Bell telephone allowed humans to communicate with a technology, but the telephone depended on wire connections and because of this, it would be fixed on top of a desk or wall (Crowley & Heyer, 2015). Succeeding the Bell telephone, advances towards a mobile hand-held communication device were developed (Agar, 2013). The advances included hand-held radio transceivers that were effective in sending and receiving communication, however, these hand-held radio transceivers had disadvantages, such as being heavy and bulky. Additionally, these devices were developed to be utilised within the military bases and did not consider how they would be used within organisations or by individuals for when they perform their daily tasks (Grillmayer, Dipl, & Wachs, 2013).

Therefore, there were attempts made to amend and rectify the disadvantages identified with the hand-held radio transceivers. Subsequently, during the 1990's there was the innovative invention of the Nokia mobile phone. The Nokia mobile phone was a weightless, hand-held, portable, and wireless device. It also had features such as; a clock, calendar and games to name a few (Goggin, 2012) This invention made a statement and impact within the history of mobile devices, as it had aspects of versatility and flexibility that allowed an individual to perform different personal activities using one device anywhere and anytime. These personal activities were inclusive of verbal and textual communication of information (Harris & Patten, 2014).

Nokia and other organisations made further advances to this mobile phone. The advances made to the mobile phone would lead to the invention of other mobile devices and services. Mobile devices that consist of features that provide the user with the ability to conduct various tasks, such as voice calls, input reminders of upcoming meetings or other events on the device calendar and other tasks. However, mobile devices are becoming dependent on wireless technology (Becher et al., 2011). Wireless technology has been associated with the use of mobile devices and allows communication on the mobile device that is free from any wires (Sharma, 2013). Examples of wireless technology include Wi-Fi and Bluetooth. Thus, wireless technologies actually enabled mobile devices.

3.3.2. The impact of wireless technology on mobile devices

The initial purpose of developing wireless communication was a result of the exorbitant costs affiliated with laying and maintaining physical wire cables used for conducting

communication through technologies such as telephones (Sharma, 2013). Mobile devices are one of the numerous technologies that primarily use wireless technology when conducting communication (Gandotra & Kumar, 2016).

In the history of wireless technology for mobile devices, the Mobile Phone Service was the initial wireless service used to transmit the vocal communication through mobile devices. However, the service was susceptible to poor vocal communication transmissions, there was a lack of security and it would have instances of unreliability (Pachauri & Singh, 2012). Amendments were made to the Analogue Mobile Phone Service with the addition of wireless features such as; General Packet Radio Service (GPRS) and Enhanced Data Rate for GSM Evolution (EDGE). GPRS allows the communication of SMS's, Multimedia Messaging Service (MMS) access to the internet, and other services. Whilst EDGE permits the transmission of high volumes of data (Pachauri & Singh, 2012).

The incorporated features improved the speed of data transfer and voice quality communication on the mobile devices. Consequently, the device-to-device communication is improved and as a result has features such as Bluetooth technology that were incorporated into the mobile devices (Gandotra & Kumar, 2016). Bluetooth technology allows wireless communication of information in a short range of space between two or more mobile devices (Bisdikian, 2001).

Literature advocates that the current and future generation of wireless technology is the World Wide Wireless Web (WWWW) which permits individuals to communicate on a wireless mobile internet using their mobile device (Sapakal & Kadam, 2013). This is a generation where the mobile devices have features such as, various artificial intelligence capabilities, which are wearable. There is also the gigabit data broadcasts that can be implemented through 65,000 connections, the connections are made through virtual private networks and other advanced features (Pachauri & Singh, 2012). Cloud Computing Resources (CCR) facilitates the implementation of these features. CCR provides the comfort of accessing and storing data and applications on an on-demand network, configurable to computing resources such as mobile devices. Mobile devices will permit day-to-day services such as mobile banking, mobile healthcare, mobile commerce and other services on the WWW (Sapakal & Kadam, 2013).

The discussion in this subsection points out that wireless technology has had an impact on the way mobile devices are used. Furthermore, users of mobile devices are becoming dependent on wireless technologies in order to communicate and perform various tasks. Thus, it will be interesting how the next generation of wireless technology will influence the use of the mobile devices.

3.3.3. The proliferation of mobile devices

In the 21st century, there is an increasing demand to maintain instant and constant communication using ICT. This is evident in the everyday life and in organisations, as communication is conducted wirelessly using ubiquitous technologies, namely mobile devices, and other forms of ICT.

Organisations utilise mobile devices to communicate and complete their tasks. Employees can import and export work-related information such as spreadsheets or word documents on their mobile devices and work on it at home. Once the employee completes the amendments on the spreadsheet, they can email it to the relevant colleague (Charbonneau, 2011). Additionally, they can receive organisational emails, make and receive client calls and perform other organisational tasks on the mobile devices (Ambika & Radha, 2012).

In everyday life, an individual can forget to communicate a message face to face to individuals, but if the individual owns a mobile device, the individual can be reminded and thereby use their mobile device to communicate the message. Another convenience of mobile devices is if one is lost in an unknown geographical area and to have the comfort of the Global Positioning System (GPS) that will direct and locate them to their destinations (Kamboj & Gupta, 2012). In some instances, one does not even need a car; there are Uber services that will assist with transportation with just one voice call or click from the mobile device (PwC, 2016). Therefore, mobile devices have a vast influence on communication, as communication is flexible, simpler and easier.

The impact of the proliferation of mobile devices could have been unintended in the initial stages of mobile device development. However, as with any technology that warrants longevity, mobile devices have adjusted and adapted so that individuals in everyday life and organisations can depend on them (Twinomurinzi & Mawela, 2014). Thus, it is evident from

the discussion within this section that the convenience that comes from the time spent interacting with and communicating using these mobile devices is undeniable.

Mobile devices have previously been used either as a personal or as an organisational device. With the pervasiveness of mobile devices, bridging the gap of separating a mobile device to be used as both a personal and organisational technology is a phenomenon (Mittleman, French, Welke, & Guo, 2013). There are different phenomena that have attempted to develop a single mobile device that can be used at work and at home. However, a distinct phenomenon that is in existence currently that uses a mobile device as a personal and organisational device, is that of BYOD.

3.4. Bring Your Own Device

Technology is constantly evolving with each passing era. As technology evolves, there are different phenomena that attempt to process, store and communicate organisational information whilst reducing costs. Thus, the evolution of technology has developed into a relatively new phenomenon called: “BYOD”. BYOD is a phenomenon that is changing the dynamics of the organisation and personal daily activities. It allows users to view mobile devices as not just mere personal devices, but multi-context devices that can be used in a personal and an organisational context (Garba, Armarego, Murray, et al., 2015). Therefore, this section discusses the phenomenon of BYOD with its advantages and disadvantages.

3.4.1. What is BYOD?

BYOD can be defined as; allowing employees to bring their own mobile devices to the organisation to be utilised for conducting organisational tasks (Madzima, Moyo, & Abdullah, 2014). Employees utilise the personally purchased mobile device to connect to the organisational network in order to access and execute organisational tasks (Loose, Weeger, & Gewald, 2013). Thus, it could be deduced that, for a mobile device to be referred to as a BYOD device, it must be purchased and owned by the employee and the employee should utilise the mobile device to gain access to the organisational information.

In most instances, since the BYOD device is purchased by the employee; the employee has the choice of choosing the type of mobile device they want to utilise. The BYOD devices are typically inclusive of smartphones, tablets and e-readers. A subsidy may be included with the adoption of BYOD in some organisations as users need to access information with limited

personal costs to their voice and data usage (Selviandro et al., 2015). The subsidy and any other specifications for the adoption and management of BYOD are namely stipulated in policies. The policy will state where and how the applicable BYOD devices can be used, which organisational information is accessible and other relevant information associated with the adoption and management of BYOD (Self & Kestle, 2013).

BYOD can also be referred to as the consumerization of ICT. The consumerization of ICT can be interpreted as communication technologies emerging within the consumer market and then spreading into organisations (Scarfo, 2012). Yevseyeva et al. (2014) advocate that the consumerization of ICT is when a user, usually an employee, owns a mobile device that can be used by both the company and for personal use (Yevseyeva et al., 2014).

The user can conduct personal tasks on the mobile device, such as access social media platforms, for example, access to Facebook; this forces the organisation to adapt its technologies to cater for both personal and organisational tasks. Additionally, the mobile devices allow an employee to be productive anytime and anywhere, as they receive sensitive organisational information on the mobile devices. Therefore, the adoption of BYOD can improve the overall organisation as tasks are completed in a timely manner through the mobile devices (Yevseyeva et al., 2014).

It is apparent from the discussion in this section, that BYOD is a phenomenon that connects the technology of mobile devices with the implementation of personal and organisational processes and tasks. Moreover, most organisations are keen in the adoption of BYOD as there are numerous and exciting benefits affiliated with BYOD.

3.4.2. Benefits of BYOD

The benefits affiliated with BYOD have permitted employees to conduct different personal and organisational tasks on mobile devices. Employees want to stay continuously connected without any constraints or time and place. The hi-tech mobile devices on the market assist employees to stay connected with limited constraints (Zahadat, Blessner, Blackburn, & Olson, 2015). Survey findings state that 74% of organisations are adopting BYOD within their respective enterprises in order to allow employees to stay connected anywhere and anytime, with the use of their hi-tech mobile devices (Yevseyeva et al., 2014).

Organisations both small and large, are adopting the phenomenon of BYOD. With the adoption of BYOD, organisations can reap its benefits. The dual-use of a mobile device for personal and organisational purposes has the following benefits:

Access: Access to organisational resources via the organisational network, allowing employees to work “anytime” and “anywhere”. Organisations are fast-paced and constantly growing enterprises, thus the technologies they incorporate should allow employees to be constantly productive and responsive. Moreover, the technologies need to be light in weight and compact enough to be moved around (Madzima et al., 2014). Additionally, when organisational tasks are conducted “anytime” and “anywhere”, this provides the organisation with a competitive edge. This is due to the lack of an employee being confined within the organisational infrastructure when completing the organisational tasks (Zahadat et al., 2015).

Increased Productivity and Innovation: The BYOD devices have the additional benefit of being able to conduct personal and organisational activities in one mobile device. Consequently, the BYOD device user becomes familiar with the device and there is minimal training needed (Twinomurinzi & Mawela, 2014). When there is minimal training required, there is increased production and innovation.

Employee Satisfaction: Employee satisfaction is seen through the convenience of using a mobile device that the employee prefers, which provides the employee with the flexibility of conducting personal and work tasks (Lebek et al., 2013).

Cost-Savings: BYOD can assist in the reduction of costs towards organisational expenses as the device is purchased and owned by the employee. There is also minimal training needed for BYOD, therefore, there are cost-savings affiliated with the implementation of BYOD (Garba et al., 2015).

Another benefit of BYOD extends to afford the employees the choice of choosing the mobile device to be used for BYOD. This can be in circumstances where an employee has an organisational owned laptop but does not have a tablet needed for conducting other organisational tasks such as receiving emails, storing spreadsheets that can be accessed at home or being able to call or SMS a client. As a result, the employee may bring their personally owned tablet to be utilised for organisational tasks (Loose et al., 2013).

Then, when the need arises for the employee with the BYOD device to gain access to organisational information, the organisation will authorise the employee through the BYOD initiative. Hence the device is personal, the employee will also be able to gain access to social media and conduct any other related personal activities on the BYOD device (Lebek et al., 2013). This allows the employee to be constantly productive whilst addressing personal activities.

With the benefits of the dual-use of the BYOD devices, there is a blurred view of when tasks can be conducted as personal and organisational. Nevertheless, employees are generally satisfied with the venture of BYOD and this is evident in the overall increased productivity whilst costs are reduced (Scarfo, 2012). However, with the benefits of the adoption of BYOD mentioned in this subsection, there are also the risks associated with BYOD. Therefore, organisations should be aware of the risks to implementation of BYOD and apply proper management.

3.4.3. Risks of BYOD

Employee demand for the implementation of BYOD leaves the organisation with minimal choice but to adapt to the changing environment (Self & Kestle, 2013). However, with the implementation of BYOD, there are risks to the organisation, particularly associated with the organisational information. The risks pertaining to BYOD include the following:

- Loss of organisational information due to information being accessed by unauthorised users through cloud computing, social engineering and other sources (Pillay, Nham, Tan, & Diaki, 2013).
- Loss of organisational information due to a lost or stolen mobile device (Dedeche, Liu, Le, & Lajami, 2013).
- Organisational information accessed, as a result of viruses, malware and phishing infiltrations or attacks through spoofed emails or URLs (Dang-pham & Pittayachawan, 2014).

Figure 3.1 below provides an illustration of some of the other risks or challenges associated with BYOD. From Figure 3.1, the cost of training and mobile application development costs are lowest challenges that are faced by organisations. This may be in relation to the user of the mobile device being familiar with their personal device and may not require any training.

Furthermore, the user may be installing software that they prefer on their personal device, at their own cost.

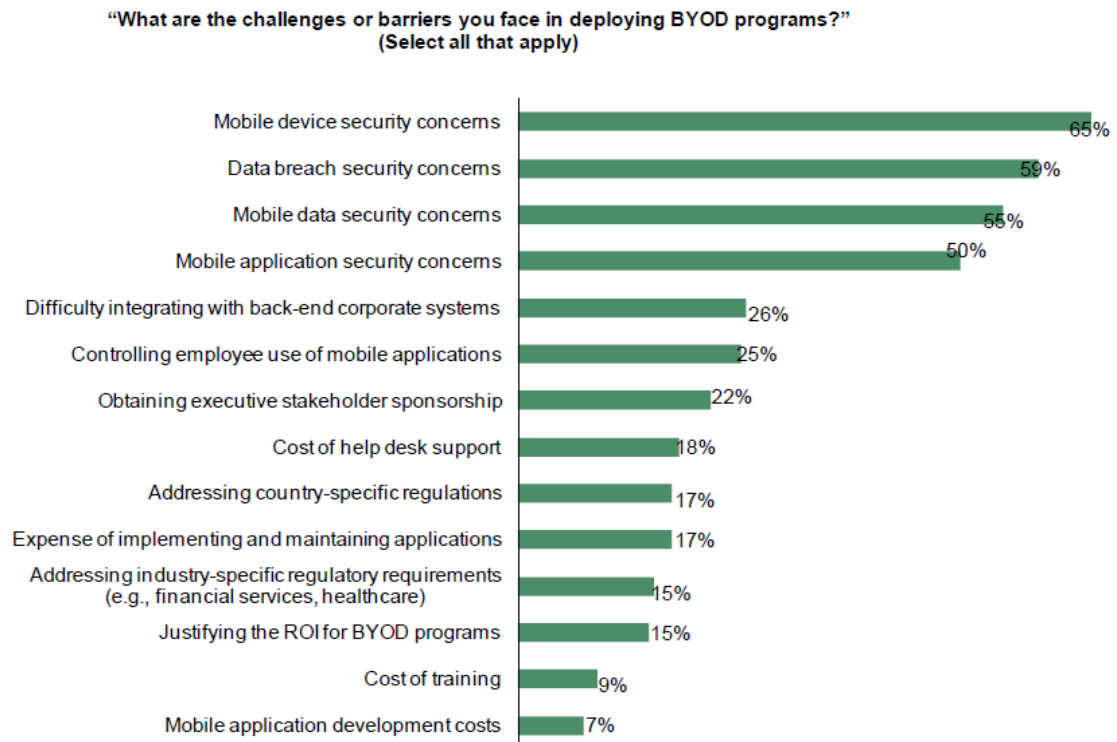


Figure 3.1: Challenges or barriers of BYOD

Figure 3.1 also provides evidence that the highest concern for organisations, should be mobile device security and data breach security, as there are assets within the organisation, namely information that could be exposed because of the risks pertaining to BYOD (Forrester, 2012). The exposure of the organisational information could harm and damage the reputation of the organisation. Therefore, from the discussion in this subsection, it is clear that the decision to implement BYOD within an organisation should attempt to consider the risks together with the benefits of BYOD.

3.4.4. BYOD within organisations

Within the organisation, there is ICT owned by the organisation. The organisationally owned ICT will be utilised to conduct most tasks. However, the organisationally owned ICT can be expensive to purchase and manage. Thus, organisations are constantly looking for ICT that

can assist them in reducing the overall costs and management associated with their ICT (Kew, Herrington, & Hooper, 2010). The adoption of the mobile devices utilised for BYOD in most organisations, has assisted organisations in reducing the costs associated with the technology as the employees purchase and manage the devices with minimal organisational influence (Botha et al., 2009). Thus, most organisations are adopting BYOD within their context (Loose, Weeger & Gewald, 2013).

The initiative to adopt BYOD is not only encouraged by organisational strategies, as employees demand the implementation of BYOD. Employees demand the implementation of BYOD, as it provides them with the flexibility of using a single mobile device in two different environments (work and home) (Scarfo, 2012). Consequently, the commitment to the utilisation of BYOD will impact the culture and behaviour of employees within the organisation, as the employees have to adapt to the changes that influence both their personal and work space. This is due to the employee being able to access both personal and organisational information in both the personal and work space (Weeger & Gewald, 2014).

When employees utilise their BYOD devices for personal and organisational purposes, the respective IT department has restricted control over the BYOD devices. Additionally, the mobile device that is utilised for BYOD is purchased by the employee and the employee is able to choose from multiple brands and devices (Hensema, 2013). As a result, the implementation of BYOD affects the IT department as there can be “unknown” BYOD devices which need to be managed. Furthermore, organisations should remain aware of the confidential organisational information being accessed through the BYOD devices (Astani, Ready, & Tessema, 2013). The information is at a risk of; data leakage through circumstances such as a lost/stolen device and hacking (Dedeche et al., 2013).

In order to cope with increasing risks associated with BYOD, there should be proper management of the BYOD devices. There are different policies and strategies that organisations can formulate in order to manage BYOD. This allows management and control over how BYOD is implemented within the organisation thereby reducing some of the risks associated with BYOD (Madzima et al., 2014).

BYOD allows organisations to stay innovative and have a competitive edge. However, with the numerous BYOD devices connecting to the organisational network, an organisation can

become overwhelmed due to the risks associated with BYOD. This is inclusive but not limited to perpetrators enticing employees to expose organisational information through malware-embedded emails sent to employee email accounts on their mobile devices. Another risk includes employees that download unauthorised software or applications that could contain malicious viruses that could harm or expose organisational information (Ghosh & Rai, 2013). Therefore, it is critical that when organisations adopt BYOD, they should implement security mechanisms to protect their organisational information.

With the existence of the phenomenon of BYOD, small organisations also referred to, as SMMEs), like most large organisations, are adopting the BYOD phenomena within their environments. However, before BYOD can be discussed in SMMEs, it is important to first discuss the unique factors associated with SMMEs.

3.5. SMMEs

The Global Entrepreneurship Monitor (GEM) South African survey report of 2015/2016 points out that the increase in unemployment is a global issue that needs to be addressed (Kew & Herrington, 2015). Consequently, to try to alleviate the rise of unemployment, individuals become entrepreneurs by using the skills and knowledge they have to start their own Small Medium or Micro Enterprise (SMMEs).. These businesses that the individuals started are normally called SMMEs (Xesha, Iwu, & Slabbert, 2014).

According to the National Small Business Amended Act No. 102 of 2004, an SMME definition is; “A separate and distinct business entity, which is managed by one or more owner(s), which predominantly conducts its business in any sector and/or subsector of the national economy”. In some countries and instances, an SMME is known as an Entrepreneur or a Small and Medium Enterprises (*SMEs*), which is the global term for an SMME (*National Small Business Amendment Act, 2004*).

SMME owners range from hawkers, to household owners, to small entity shop owners. The owners usually provide products and services in the homes or rent a small room in a large infrastructure for their business. There are different challenges which affect SMMEs, such as financial issues or limited/lack of ICT resources. However, SMMEs are viewed as contributors to the growth of the economy and assist in creating jobs for other unemployed individuals (Abor & Quartey, 2010).

SMMEs, like any organisation, develop in different phases. Churchill and Lewis (1983) describe five phases of SMME development in Figure 3.2. The five phases begin with the initial stage (Growth through creativity), where the owner uses their own skills and knowledge to create a business. The business will go through other phases of development, and if successful, will reach the last stage of development (Growth through collaboration). The last stage displays that the SMME has matured into an organisation with different spectrums of employees working together in a well-established enterprise (Lewis & Churchill, 1983).

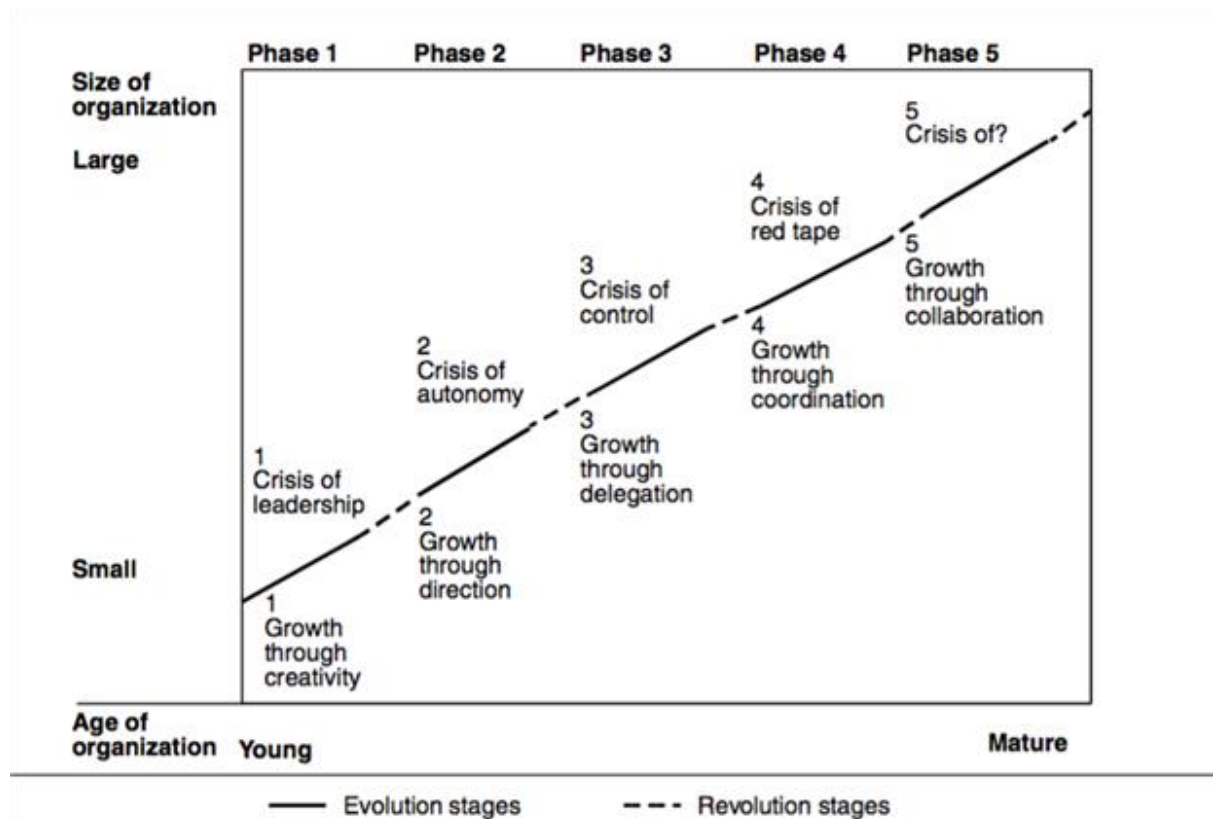


Figure 3.2: Five phases of SMME development

A detailed description of the five phases is as follows:

Phase 1 - Existence stage (Survivalist enterprises): In the early phases of the SMME, there is an individual owner. The owner has minimal training or asset investments. Nevertheless, the owners will provide products and services that will attract potential clients. Some owners may have enough money to employ an administrator who will manage the administration aspect of the enterprise. The enterprise operates in the informal sector of the economy.

Phase 2 - Survival stage (Micro Enterprises): The SMME enterprise has managed to sell products or provide services and has a client database with regular customers. Profit from the products and services allows the enterprise to grow and the owner is able to hire more employees. The employees employed are usually the owner's family and can range from one to five employees. The employees have basic business skills and training and the enterprise is an informal enterprise with no licence or formal business infrastructure.

Phase 3 - Success stage (Very small enterprises): The enterprise is stable at this stage and the owner begins to register the enterprise into the market that contributes to the economy. The enterprise consists of ten paid employees or less, such as self-employed artisans (electricians) and other professionals. The enterprise is at a critical stage as it needs to research how it can sustain itself with the limited resources gained or it could risk liquidation.

Phase 4 - Take-off stage (Small enterprise): The owner of the enterprise may be providing guidance but not managing the enterprise at this stage. The small enterprise has now grown to the capacity of employing approximately 100 employees. The enterprise has a fixed business premises and will likely adapt its products and services to focus more on the customer's needs, rather than enterprise growth.

Phase 5 - Resource mature stage (Medium enterprise): During this stage, the enterprise can manage without the owner's involvement. The owner and enterprise are reasonably separate, both financially and operationally. The focus of the enterprise will be on enterprise upgrades and maintenance. Moreover, at this stage, the enterprise has approximately 200 employees. The enterprise operates from fixed infrastructure and is now a well-established enterprise (Lewis & Churchill, 1983).

As seen from the discussion, there are different phases to the development of an SMME. Although SMMEs can begin as small enterprises, they can develop into successful structured and financially stable organisations. However, with the success of SMMEs, there are also challenges that could influence the development of the SMME.

3.6. Challenges of SMMEs

Large organisations face different challenges but are able to manage because of the vast assets and segments within their organisation. Therefore, the vast assets and segments will assist the large organisations to remain innovative and grow (Mervyn, 2009). Within SMMEs, there is

a lack of vast assets and segments that can assist the enterprise to grow. An SMME can consist of a single employee or entrepreneur trying to develop a business for their survival, particularly in the existence stage of the enterprise. Additionally, the owner may have limited skills and knowledge to strategically grow and manage their enterprise (SAICA, 2015). Soni, Cowden and Karodia (2015) conducted a study on the various challenges that face SMMEs, particularly SMMEs in South Africa. Below are some of the findings from that study:

Education and skills: SMME owners are usually uneducated in the trait of business. Thus, they lack the knowledge and skills acquired from an educational institution. Documentation of the running of the enterprise, finance and general management of the enterprise might not be part of the SMME owner's strategy when they initiate the business. According to the GEM South African Survey Report of 2015/2016, owners of SMMEs are more likely to create self-employment opportunities for themselves. The decline in job growth aspirations may be linked to the increase South Africa's rigid labour regulations and poor skilled or uneducated labour (Kew & Herrington, 2015). Therefore, if there is a lack of the consistent management of the enterprise, skills and business knowledge, the likelihood of the SMME's success is futile.

Location: The geographical location of the SMME is important when an SMME wants to succeed. A good geographical location assists the SMME to have regular clients and potential clients in immense numbers, as the location might be in a busy area, such as a shopping centre. With some of the SMMEs starting their enterprise within their households or any geographical location that is cost effective, it might be difficult for the SMME to grow in the number of clients and its revenue.

Registration: Most SMMEs are often too small to register their businesses. Those that can afford to register their enterprise will do so. However, maintaining the enterprise's registration can be expensive for an SMME, as the registration documents need updating yearly. Therefore, a budget for registration is required each year by the SMME. Furthermore, although the owner may be financially stable, the owner can have limited or have acquired no formal education and may have trouble understanding the documentation for the process of registration. The new Companies Act of 2009 tried to provide a simpler registration process

but the act lacked in reducing the costs affiliated with the registration (*Companies Act*, 2009). Thus, most SMMEs find it a challenge to register their enterprises.

Tax: When the SMME is registered, it will be liable to pay tax. Within South Africa, the tax is paid to the South African Revenue Service (SARS). When the SMME enterprise does not fulfil their obligation of payment towards tax, there can be penalties and fines towards the enterprise. With the already exorbitant amounts paid towards tax, this can be a debilitating challenge towards the growth of the SMME.

ICT: ICT is important in any organisation in this modern day. However, organisations such as SMMEs have limited budgets to contribute towards purchasing ICT resources. Furthermore, unlike large organisations, which have an IT department that handles the ICT related issues such as information security incidents and attacks, hardware and network issues, an SMME cannot financially afford such an IT department. Moreover, a lack of knowledge on the usability and effectiveness of the ICT in assisting the SMME may prevent SMMEs from incorporating ICT within their enterprises (Soni, Cowden, & Karodia, 2015).

There are government initiatives that are available to assist in the challenges that SMMEs have. Most of these government initiatives provide financial assistance to the SMMEs. Within South Africa, departments such as the Department of Trade and Industry (DTI) lead the government initiatives that assist SMMEs. DTI encompasses multiple programs, which include, but are not limited to the Incubation Support Programme me (ISP). ISP is a programme me that incorporates the partnerships between SMMEs, the private sector and government. These partnerships permit the growth and development of all the sectors, whilst growing the economy through incubator programs. ISP offers mentorship to organisations, business development services and other related business product and service development programme. The financial investment offered by ISP can be a maximum of ten million rand over a period of three years (Khan, 2014).

This section mentions some of the challenges that limit the growth and success of SMMEs as they compete to grow into the large organisations. With assistance from government programmes, the SMMEs can focus on the management of the organisation, without the hassles of challenges such as finances.

The assistance of government programmes for SMMEs provides them with the financial capability that allows them to purchase basic ICT for their enterprises. Nevertheless, SMMEs are persistent in their aim to find new strategies such as cleverly using technology, which can assist them to develop into large enterprises. With the emergent phenomenon of BYOD, SMMEs are adopting BYOD within their respective enterprises as there are benefits of BYOD such as the mobile device being purchased by an employee and not the SMME enterprise. However, SMMEs should be aware that there are also disadvantages and risks affiliated with BYOD (Devos, Landeghem, Deschoolmeester, & Devos, 2012).

3.7. BYOD and SMMEs

The proliferation of mobile devices has permitted the phenomenon of BYOD, which is being adopted by both large and small (SMME) enterprises. The benefits of the implementation of BYOD particularly in an SMME could assist in reducing the limited budgets and costs affiliated to the SMME resources. This is due to circumstances such as the cost of purchasing the devices and the maintenance of the BYOD devices is handled by the employee (Ghosh & Rai, 2013). Therefore, BYOD is a phenomenon that could assist SMMEs to become productive with limited resources.

With this in mind, the adoption of BYOD within SMMEs will reap some benefits, but benefits should be weighed against the implications of the adoption of BYOD. For example, when an SMME implements BYOD, limited budgets, resources and education should not be the only issue the SMME fixated on, but every aspect affiliated with the phenomenon must be taken into account (Arthur, 2012).

The small stature and limited resources of SMMEs make SMMEs vulnerable to weaknesses such as the exposure of their information to unauthorised users. It is common that incidents of breaches to the SMMEs network and other resources develop. The pressure for the maintenance of existing SMME resources provide difficulties in monitoring other factors such as the protection of the enterprise's information. Amongst others, the protection of the SMMEs information, whilst using these mobile devices for BYOD (Okello-Obura & Matovu, 2011).

Consequently, caution must be applied by the SMMEs as they can become easily susceptible to the risks associated with BYOD. A study conducted on SMMEs in the Twente region in the

Netherlands found that 38% of SMMEs see ICT related security incidents damaging and the biggest risk to their ICT infrastructure. It was found that, although SMMEs reported minimal security incidents, it was probable that the risks were masked by hackers who had broken into the ICT infrastructure (Ommen, 2014). Because of this, SMMEs who implement BYOD may face some challenging risks.

Nevertheless, there are BYOD initiatives such as; strategies, recommendations and frameworks outlined in literature. Before embracing these BYOD initiatives, SMMEs should understand their particular requirements and what is appropriate in their environment. The protection of the information related assets in the SMME will need guidance from documents such as policies. The policy would include all the guidelines on how the SMMEs need to protect the information when implementing BYOD, bearing in mind the resources in the SMME (Garba, Armarego, & Murray, 2015). Therefore, when there is a guidance for BYOD within SMMEs, the SMME could manage BYOD more effectively.

This section highlighted that BYOD is associated with benefits that assist the SMMEs immensely in growing. However, there is organisational information harboured within the mobile devices utilised for its implementation (Allam & Flowerday, 2011). With the threats and risks that affect the information, SMMEs should harbour a culture of protecting their information at every avenue. Thus, proper BYOD management is imperative in SMMEs if they utilise BYOD as part of their business strategy.

3.8. Conclusion

The proliferation of the use of mobile devices makes it difficult for organisations to stay clear from adopting the mobile devices into their environments. However, mobile devices are not the only communication technologies utilised throughout history for communication. Thus, this chapter discussed the development and history of communication technologies. Following that discussion, the context of mobile devices was discussed in detail. Subsequently, the discussion of the emergence and growth of the phenomenon of BYOD endorsed by most if not all organisations were emphasised.

This chapter further discussed the context of SMMEs. SMMEs face challenges that limit of stunt their growth and success as they compete to grow into the large organisations. As a result, the challenges of SMMEs were emphasised. One of the challenges of SMMEs was

their inability to incorporate technologies into their enterprises because of financial constraints. This resulted in the SMMEs adopting the phenomenon called BYOD. Consequently, a discussion on BYOD and SMMEs concluded the chapter.

The next chapter discusses the research design for this study. Within the chapter, the research paradigm, research process and the contextualised process are emphasised. Thereafter, there is a closing discussion on the research methods of this study.

Chapter 4: Research design

4.1. Introduction

Literature indicates that BYOD is a relatively new phenomenon that requires proper management from most organisations, specifically in SMMEs. Furthermore, the implementation of the BYOD phenomenon is associated with organisations that are confronted with real-life risks, as most SMMEs are implementing BYOD without proper management of BYOD. With BYOD being a relatively new phenomenon, there is a need to understand the context of BYOD, the real-life risks that BYOD poses and how organisations experience BYOD within their environments.

From the literature studied, it is clear that BYOD poses a real-life problem in modern organisations, including SMMEs. To address the associated problem, proper management of this situation is imperative. For this reason, a proposed management framework to effectively manage BYOD will be developed. This proposed management framework will be in the form of an artefact. From the above, it is clear that the paradigm of design research seems logical to address this problem.

This chapter provides a discussion on the research paradigm utilised in this study. Following the discussion on the research paradigm, the research process followed and thereafter, a discussion on the contextualised research process. Finally, the research methods used are emphasised.

4.2. Research Paradigm

The proposed overarching research paradigm for this study is that of design research. In particular, design-oriented IS research seems appropriate, as the research problem will be addressed within the field of IS. Design-oriented IS research provides researchers with guidelines for addressing a real-life problem they identified. The aim of design-oriented IS research is to develop an artefact through an iterative process, that can be implemented in organisations Österle et al. (2011) proposes four phases for the development of the artefact in design-oriented IS research. The first phase is an analysis phase where the problem is analysed. The second phase is a design phase where solutions to the problem are identified and a particular draft artefact as a solution is developed. The third phase is an evaluation phase which consists of the refinement and validation of the artefact against specified

objectives, methods etc. The fourth phase is the diffusion phase where the solution is finalised and passed on (Österle et al., 2011). Figure 4.1 illustrates the four-phased process:

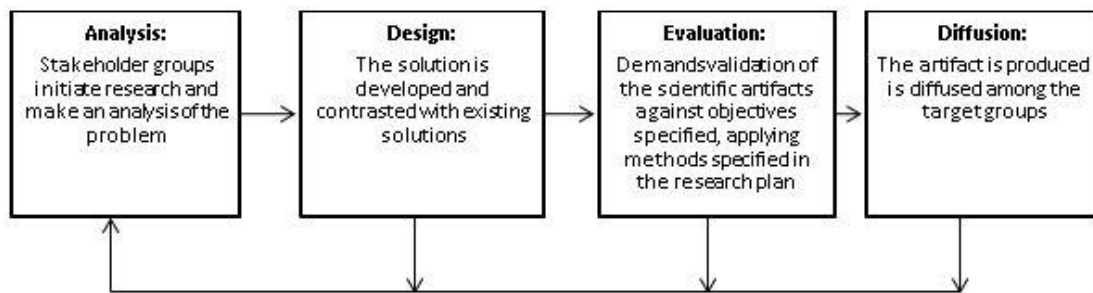


Figure 4.1: Four-phased approach for design-oriented IS research

The four phases of design-oriented IS research are ideally suited to this study. They are appropriate in that they allow the artefact, towards solving the research problem, to be addressed within a specific context (that of BYOD in SMMEs) to be applicable to a particular class of stakeholders. Design-oriented IS research expects the developed artefact, for BYOD in SMMEs in this case, to be validated before it can be diffused to the class of stakeholders.

Design-oriented IS research encompasses four basic principles. The four basic principles for design-oriented IS research are:

- **Abstraction:** Each artefact must be applicable to a class of problems.
- **Originality:** Each artefact must substantially contribute to the advancement of the body of knowledge.
- **Justification:** Each artefact must be justified in a comprehensive manner and must allow for its validation.
- **Benefit:** Each artefact must yield benefit – either immediately or in the future – for the respective stakeholder groups.

These principles form the foundation of design-oriented IS research and need to be met satisfactorily. The principles are appropriate for this study as a real-life problem currently experienced in SMMEs is BYOD and BYOD has real-life risks associated with it. There is not only one SMME that experiences the real-life risks associated with BYOD but most SMMEs (Kew, Herrington, & Hooper, 2010). Once the solution artefact is completed, it will need to be validated on whether it is appropriate for the SMME environment.

In this section, the four phases of design-oriented IS research together with its underlying principles are discussed. As design-oriented IS research provides very limited process support, it is imperative that alternative support is identified to assist in the execution of the individual phases of design-oriented IS research. Design-based research is one alternative approach, within the design research paradigm that can assist with more detailed process support. This will be discussed in the next section.

4.3. Research process

The research study is conducted in the field of IS and the intention of this research study is to design an artefact in the form of a framework to address a specific real-life problem. As a result, design-oriented IS research has proved to be ideal to use. However, design-oriented IS research does not provide detailed process support on how to execute each of the four phases. For this reason, design-based research has been identified to assist specifically, because, design-based research has a well-specified research process associated with it. Design-based research also utilises four phases that are very similar to the four phases of design-oriented IS research. Therefore, design-based research is ideal to use in combination with design-oriented IS research. Table 4.2 provides an illustration of the four phases of design-based research (Herrington, Mckenney, Reeves, & Oliver, 2005):

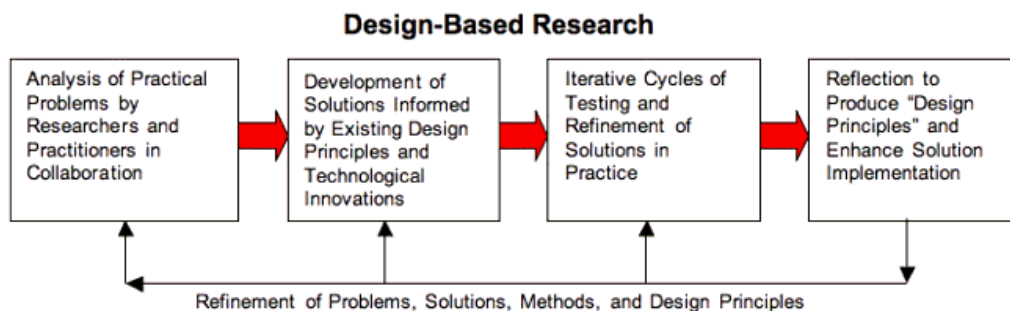


Figure 4.2: Four-phased approach for design-based research

Design-based research consists of various elements associated with each of the four phases. The elements provide the necessary process guidance on what should be done during each of the four phases. Table 4.1 below captures the elements that provide the guidance on the research process to be followed through each of the phases of design-based research, which is interlinked with design-oriented IS research. Therefore, this research process provided by

design-based research can be used because design-oriented IS research also provides the researcher with the freedom to utilise the approach they require as applicable.

Table 4.1: Research process (Herrington et al., 2005)

Phases	Element	Position in research
Phase 1: Analysis of practical problems by researchers and practitioners	Problem statement	An initial research problem is identified primarily through literature. After identifying the problem and consultation with practitioners (stakeholders), the problem statement is refined and finalised.
	Consultation with researchers and practitioners	
	Research questions/objectives	When the problem statement is finalised, research questions/objectives are set for this research. The research questions/objectives are dependent on literature reviews.
	Literature review	After the problem and the research questions/objectives have been set, a further literature review is conducted on this specific research.
Phase 2: Development of solutions informed by existing design principles and technological innovations	Theoretical framework	Based on the literature review that concluded phase 1, an initial theoretical framework to address the problem is drafted. Along with the draft of the initial theoretical framework, a number of principles are identified by which the eventual artefact can be validated against. These principles act as a guide to the design of the intervention.
	Development of draft principles to guide the design of the intervention	
	Description of	Following the initial draft of the

	proposed intervention	theoretical framework and with the principles set, the intervention will be in the form of an artefact meeting the set principles.
Phase 3: Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteration)	
	Participants	Participants acting as stakeholders need to be identified.
	Data collection	Data will be collected from the stakeholders based on initial theoretical framework and intervention.
	Data analysis	This data is analysed and the intervention will be adapted according to the analysed data received from the stakeholders.
	Implementation of intervention	
	(Second and further iterations)	Second and further iterations will be implemented, with data collection and analyses with the stakeholders, until the stakeholders are satisfied.
	Data collection	
	Data analysis	
Phase 4: Reflection to produce “design principles” and enhance solution implementation	Design principles	After the stakeholders have accepted the intervention in the form of an artefact, the intervention needs to be validated against the design principles set in phase 2. This intervention takes place with the second

	Design artefact (s)	<p>set of stakeholders</p> <p>Following the validation response from the second set of stakeholders, the artefact is finalised.</p>
	Professional development	<p>When the artefact is finalised, it is diffused amongst the class of stakeholders.</p>

From the discussion in this section, it is clear that the goals of design-oriented IS research and design-based research are very similar and can be utilised supporting each other. As a result, this study will make use of design-oriented IS research as the overarching research approach, and utilise the research process associated with the four phases associated with design-based research. This will result in a contextualised research process.

4.4. Contextualised research process

The aim of this study is to formulate a framework (artefact) for BYOD that can influence the way an SMME environment manages BYOD. The formulation of the framework must consider the context of BYOD in SMMEs, as it is the main stakeholder of this study. Thus, it is important to contextualise the generic research process espoused in Table 4.2 for the SMME environment where this research is positioned. The developed framework should yield results that are beneficial to the municipality. In the previous section (section 4.3), Herrington et al. (2005) tabulated the research process for the implementation of the four phases of design-based research. Table 4.2 below provides a table.

Table 4.2: Implementation of the research process

Phases	Element	Position in the research
Phase 1: Analysis of practical problems by researchers and practitioners	Problem statement	BYOD is a phenomenon that can cause information related risks in SMMEs
	Consultation with	A District Municipality was

	researchers and practitioners	identified as the SMME and the IT personnel from this District Municipality were identified as stakeholders
	Research questions/objectives	<p>Primary research objective:</p> <p>To formulate a framework towards governing information related risks associated with the rollout of BYOD in an SMME environment</p> <p>Secondary research objective/s:</p> <ul style="list-style-type: none"> • To study the information related risks associated with BYOD in a typical SMME environment • To identify governance related sources currently in place for BYOD that could be utilised in an SMME environment • To formulate a governance-orientated solution towards mitigating information related risks of BYOD in an SMME environment
	Literature review	Document analysis
Phase 2: Development	Theoretical framework	Investigate theory available in

of solutions informed by existing design principles and technological innovations		the context of BYOD in SMMEs
	Development of draft principles to guide the design of the intervention	<ul style="list-style-type: none"> • Investigate the context of BYOD • Investigate the impact of BYOD in SMMEs • Formulate a framework to manage BYOD in SMMEs
	Description of proposed intervention	Influence the management of BYOD in SMMEs by providing a BYOD framework
Phase 3: Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteration)	
	Participants	IT personnel from this District Municipality
	Data collection	Mixed research methods (Literature review, surveys)
	Data analysis	Analysis of data on BYOD with the benefits and challenges
	Implementation of intervention	First draft of the framework (artefact)
	(Second and further iterations)	To be determined
Phase 4: Reflection to produce “design	Design principles	<ul style="list-style-type: none"> • Scalability – The contribution should be

principles” and enhance solution implementation		scalable for an SMME environment. <ul style="list-style-type: none"> • Utility – The contribution should be usable in the SMME environment. • Efficacy - The contribution should be efficient and developed with the SMME environment in mind. • Quality – The contribution should be formulated to provide value in an SMME environment.
	Design artefact (s)	Finalisation of a BYOD framework
	Professional development	Diffusion of the BYOD framework that will assist SMMEs in their management of BYOD

Table 4.2 provides a brief description of how each phase was implemented in this study by categorising each of the elements in each phase. A more detailed description of the implementation of each phase will follow in the next chapter. The research methods used within each of the phases is briefed in the next section.

4.5. Research Methods

The design-oriented IS research approach used in this study allows the researcher the freedom to choose the most appropriate methods. Table 4.3 provides the research methods used by the researcher in this study.

Table 4.3: Research methods

Research method	Description of research method	Phase
Literature review	A literature review is used to gain knowledge on a certain topic by researching previous literature (Boote & Beile, 2005).	Phase 1: The literature review was used to identify the problem associated with BYOD and identify research questions/objectives. Phase 2: A literature review was used to assist in drafting the initial theoretical framework that would be used to assist in addressing the problem identified with BYOD.
Survey	Surveys gather data from one to many sources and the data gathered must be neutral views of individuals in a population (Owens, 2002). There are different types of surveys i.e. observation, interviews etc. but the most commonly used form of survey is a questionnaire (Vaus, 2002).	Phase 3: Data collection is conducted with the stakeholders specifically, through survey questionnaires and semi-structured interviews. Phase 4: The intervention in the form of an artefact (framework) was validated with the use of survey questionnaires.

Mind map	A mind map is also known as “brain map” or “mental map” was developed by Tony Buzan during the 1970s. It can be defined as an outline with ideas and pictures radiating out from a central concept (main idea). From the central concept key ideas radiate out, like the branches of a tree (Davies, 2011).	Phase 3: The mind map was used in the refinement process of the artefact.
Focus group	A definition for a focus group is as follows; “ <i>a group of interacting individuals having some common interest or characteristics brought together by a moderator, who uses the group and its interaction as a way to gain information about a specific or focused issue</i> ” (Masadeh, 2012).	Phase 3: A focus group was used in the refinement process of the artefact. Phase 4: A focus group exercise was using during the validation process of the artefact.

As per Table 4.3, in phase 1, it is clear that a literature review will be used to identify the initial real-life problem. Furthermore, the literature review will be used in phase 2, to base the foundation for the initial theoretical framework. While working with the stakeholders, data will be collected in the form of surveys in phase 3 and phase 4. The data collection and data analysis will assist in developing the initial theoretical framework, in phase 3. The initial draft of the theoretical framework will go through rigorous cycles of refinement with the use of surveys, a mind map and focus groups, in phase 3 and 4.

4.6. Conclusion

This chapter discusses the research design used in this study. In the discussion, design-oriented IS research was identified as the appropriate research approach, as the research problem is addressed within the field of IS. Design-oriented IS research consists of four phases that are used to address the research problem. However, the four phases specified in design-oriented IS research do not provide detailed process guidance on how to execute each of the four phases. Therefore, this chapter discussed the four phases and elements of design-based research in the research process.

The discussion of the research process revealed that the four phases of design-oriented IS research and design-based research are very similar and can be utilised in supporting each other. As a result, the four phases of design-oriented IS research and design-based research were contextualised and a discussion of the contextualised research process occurred. Thereafter, a brief discussion on the research methods used in this research study concluded the chapter.

The contextualised research process discussed within this chapter provides brief details on the implementation of each phase of the research process. Therefore, the next chapter will provide a detailed discussion of the process to the development of the artefact.

Chapter 5: The development of the BYOD Management Framework

5.1. Introduction

A survey report conducted by Ghosh and Rai (2013), found that 21% of organisations provide employees with mobile devices for BYOD, however, the management of the device is the employee's responsibility (Ghosh & Rai, 2013). Thus, the organisational information contained on the BYOD device is susceptible to security breaches and risks that the organisation might be unaware of.

The inadequate management of mobile devices by employees is further seen in reports such as, the Norton Report for the year 2013, which reports that 26% of smartphone users do not have any mobile security software. Additionally, 36% BYOD users have no BYOD policy that they have to abide by within their respective organisations ("2013 Norton Report," 2013). Therefore, the findings and risks mentioned in the report by Gosh and Rai (2013) and the Norton Report, affirm that organisations are blindly adopting BYOD with little proper management associated. Thus, this management problem is the core of the research problem to be addressed.

The previous chapter discussed the research design for this study. In the research design discussion, a research process consisting of four phases was deduced to develop an artefact as a contribution to addressing the identified problem. In this research, the identified research topic is that of the BYOD phenomenon that is associated with information related risks. In an earlier chapter, Chapter 2, it was emphasised that the information related risks of BYOD affect not only the; CIA of the information in the organisation, but could harm the reputation of an organisation, which would be hard to recover. Thus, in order to try to manage the problem of the information related risks associated with BYOD this study proposed to develop a BYOD Management Framework, an artefact, as the research contribution. The development of the BYOD Management Framework is discussed in this chapter.

Taking into regard the above, this chapter will begin with a discussion on the identified frameworks for BYOD currently in the literature. Leading the discussion on the BYOD

Frameworks, this study will evaluate and compare each framework to determine whether it will contribute towards the development of the BYOD Management Framework.

5.2. Phase 1: Frameworks for BYOD

Table 5.1: Phase 1 of the research process

Phases	Element	Position in research
Phase 1: Analysis of practical problems by researchers and practitioners	Phase 1.1: Problem statement	An initial research problem is identified primarily through literature. After identifying the problem and consultation with practitioners (stakeholders), the problem statement is refined and finalised.
	Phase 1.2: Consultation with researchers and practitioners	
	Phase 1.3: Research questions/objectives	When the problem statement is finalised, research questions/objectives is set for this research. The research questions/objectives are dependent on literature reviews.
	Phase 1.4: Literature review	After the problem and the research questions/objectives have been set, a further literature review is conducted on this specific research.

In Table 5.1, Phase 1 of the research process requires the researcher to identify the research problem together with the research objectives. As a result, a literature review was conducted to identify the research problem. This research problem was stated in both Chapter 1 and Chapter 2. Following the identification of the research problem, the practitioners (stakeholders) were identified and consulted to assist the researcher in finalising the research problem. Chapter 1 and Chapter 3 provide a discussion on the identified stakeholders. Following this, analyses of the literature review permitted the researcher to formulate the

research objectives of this study. With the formulation of the research problem, the identification of the stakeholders, and the research objectives set, Phase 1 was concluded.

5.3.1. Phase 2: Identified existing frameworks for BYOD

Table 5.2: Phase 2 of the research process

Phases	Element	Position in research
Phase 2: Development of solutions informed by existing design principles and technological innovations	Phase 2.1: Theoretical framework	Based on the literature review that concluded phase 1, an initial theoretical framework to address the problem is drafted. Along with the draft of the initial theoretical framework, a number of principles are identified by which the eventual artefact can be validated against. These principles act as a guide to the design of the intervention.
	Phase 2.2: Development of draft principles to guide the design of the intervention	
	Phase 2.3: Description of proposed intervention	Following the initial draft of the theoretical framework and with the principles set, the intervention will be in the form of an artefact meeting the set principles.

Phase 2, espoused in Table 5.2, guides the development of an initial draft of a theoretical framework through relevant design principles and existing technological innovations. This section and the section that follows, will discuss the existing technological innovations and the associated design principles.

Phase 2.1: BYOD Security Framework:

BYOD is an emerging phenomenon, thus, there are various technological innovations (frameworks) currently in existence in the literature to manage BYOD. This study analyses four prominent existing frameworks identified in literature for BYOD. The first framework

identified is the BYOD Security Framework (Zahadat et al., 2015). This framework is divided into seven phases. A brief description of each phase follows:

Plan: There should be an analysis of the organisation in order to plan on what is efficient for the management of BYOD in the particular organisation. The plans should also include the identification of the relevant users that will adopt BYOD and the organisational information they will access.

Identify: The mobile devices utilised for BYOD should be registered, approved, and provided with the appropriate security.

Protect: The appropriate security mechanisms in place should include the protection of the organisational information.

Detect: The organisation should prevent, or respond to and recover from, intentional or unintentional threat events.

Respond: There should be a response to any threats that occur within the organisation.

Recover: The organisation must be able to recover from any event that occurs.

Assess and Monitor: An organisation should assess and monitor the value and competence of the BYOD security programme (Zahadat et al., 2015).

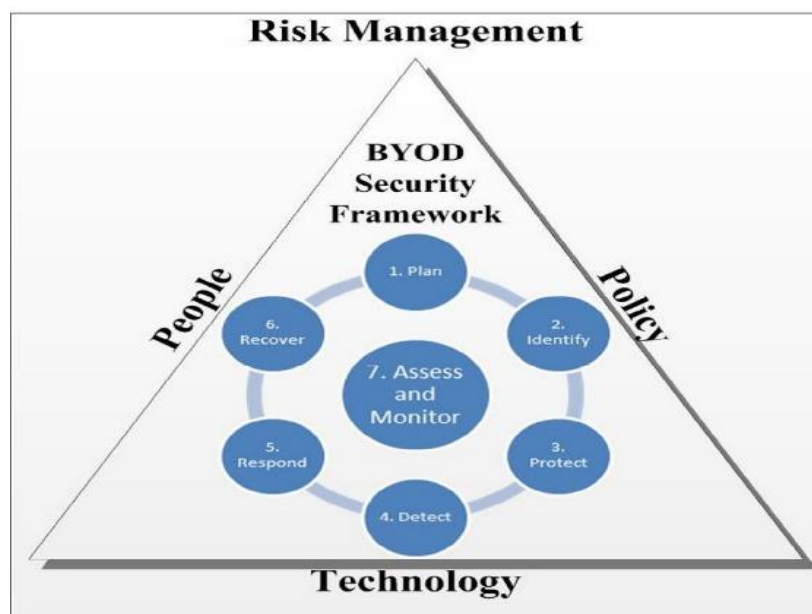


Figure 5.1: BYOD Security Framework (Zahadat et al., 2015)

Figure 5.1 provides a graphical representation of the seven phases of the BYOD Security Framework. The seven phases are encompassed by three pillars, that of; people, technology and policy. The purpose of the BYOD Security Framework is to provide a foundation for a BYOD security programme whilst incorporating a risk management strategy (Zahadat et al., 2015).

BYOD framework for a management system:

The second framework, namely the BYOD framework for a management system, manages BYOD by referring to the ISO/IEC 27000-series for guidance. The BYOD framework for a management system consists of three steps (Brodin, 2015b). The three steps are visualised in Figure 5.2 and are concisely described as follows:

Analysis: The organisation determines the relevant issues within the organisation, which affect the protection of the organisational information.

Design: Further analysis is conducted and there is the development of strategies that will assist in addressing the issues that hinder the protection of the organisational information. Existing policies are updated.

Action: The organisation performs a risk assessment. When the risk assessment is completed, the strategy can be implemented.

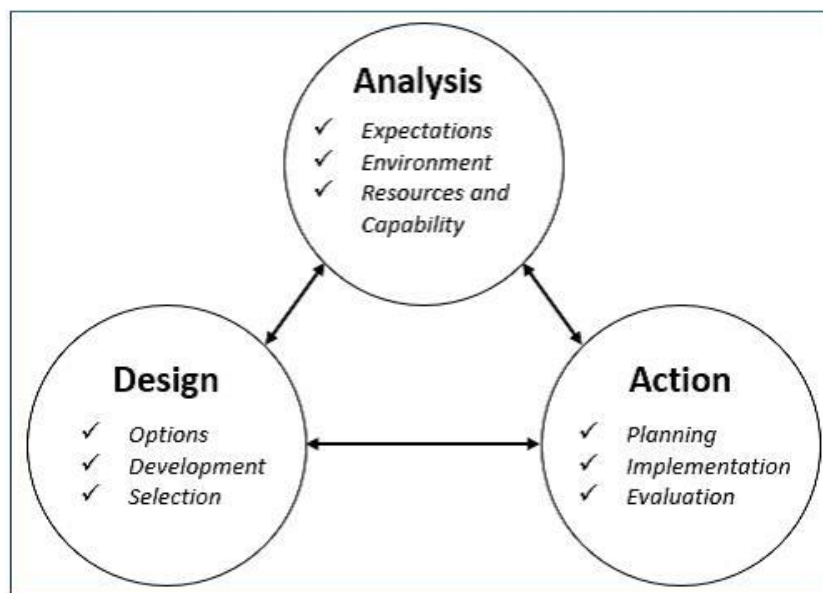


Figure 5.2: BYOD framework for a management system (Brodin, 2015b)

The BYOD framework for a management system provides a strategic way of thinking when an organisation adopts BYOD. The three steps provided in the framework, permits the organisation to formulate a solution that will be applicable to that specific organisation (Brodin, 2015b).

BYOD privacy and culture governance framework:

The third framework analysed in literature is the BYOD privacy and culture governance framework. This framework maps the organisational culture and privacy concerns within the organisation. Once the mapping is complete, a policy is developed (Selviandro et al., 2015). The components prescribed in the framework are as follows:

- Determine the culture within the organisation by investigating how the employees' interpretation of the current organisational culture.
- Determine the characteristics that the organisational culture is based on.
- Identify the privacy concerns within the particular organisation.
- Determine the privacy concerns of the employees.
- Conduct an assessment of the privacy concerns of the employees.
- Develop a policy that takes account the findings from the privacy concern assessment.
- Implement cloud management control on cloud products and services utilised for BYOD whilst taking into account the organisational culture.

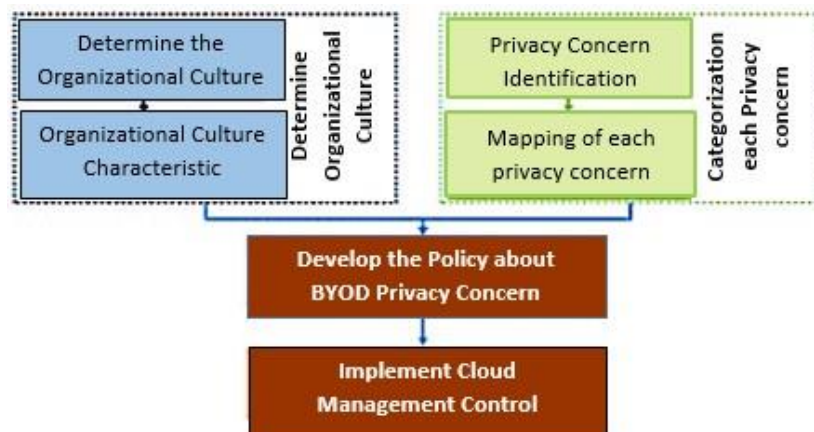


Figure 5.3: BYOD privacy & culture governance framework (Selviandro et al., 2015)

In Figure 5.3 the relationships of different components of the framework are diagrammed. The purpose of the framework is to determine if organisations benefit in the implementation of BYOD when organisational culture and cloud management control is adapted (Selviandro et al., 2015).

Enterprise and BYOD space BYOD Security Framework:

The enterprise and BYOD space BYOD Security Framework was formulated to protect the enterprise networks when BYOD is implemented. The represented framework is divided into two sides; the Enterprise side and the BYOD side. Below is a brief description of each side:

Enterprise side: Includes the corporate resources and device management. Leading from the corporate resources is the network access controls. The network access controls manage the networks that are utilised for BYOD. The networks are separated into the personal space and enterprise space.

BYOD side: The separation of the networks utilised for BYOD allows the organisation to provide the functions that assist in the corporate space which is separate from the personal space. The personal space consists of the user's personal mobile device applications and other personal information. The corporate space consists of the corporate applications, security policies, corporate information and the security mechanisms for the protection of the corporate information (Wang et al., 2014).

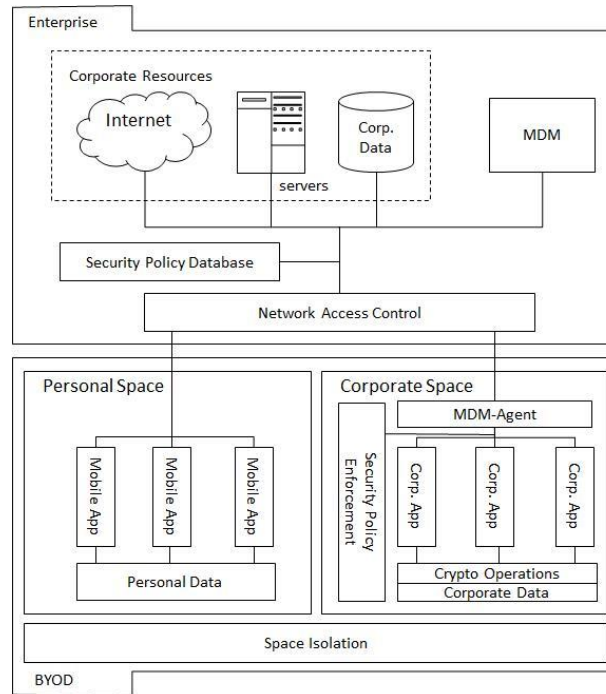


Figure 5.4: Enterprise and BYOD space BYOD Security Framework (Wang et al., 2014)

The enterprise and BYOD space BYOD Security Framework is presented in Figure 5.4. The framework provides protection to the organisational information by separating the network spaces that a BYOD user can access into enterprise space and BYOD space. This permits BYOD users to work in controlled and protected spaces (Wang et al., 2014).

The BYOD frameworks discussed in this subsection are similar in their intention of managing BYOD. Although, it is apparent that they are different in the way they are formulated and implemented. The differences between the described BYOD frameworks is discussed in the next subsection.

5.3.2. Evaluating the existing frameworks for BYOD

BYOD is a phenomenon that warrants constant management if organisations want its seamless integration whilst limiting risks to their information. The previous subsection discussed four existing frameworks from literature. Furthermore, it was pointed out that these existing BYOD frameworks have differences amongst them, however, their intent is to manage BYOD within organisations. This subsection will provide a critical evaluation of these four BYOD frameworks.

Each of the four existing frameworks in literature have their own benefits and when compared to each other, there are aspects relevant to be utilised when developing the contribution framework (artefact) for this study. Furthermore, the observation findings from the four frameworks provide elements that can be deemed as missing from the frameworks. Table 5.3 tabulates the relevant aspects and missing elements following a critical analysis of the four existing frameworks from literature.

Table 5.3: Evaluation of the existing BYOD frameworks

Frameworks	Aspects relevant to the framework to be developed	Missing elements
BYOD Security Framework (Zahadat et al., 2015)	<ul style="list-style-type: none"> - Understands the business environment. - Registers BYOD devices. - The organisation has measures for device and information protection. - The framework provides an aspect for continuous security monitoring. 	<ul style="list-style-type: none"> - The framework consists of ICT technical aspects, such as programing code for governing BYOD devices, which could too technical for some organisations. - The SMME environment is not cited.
BYOD framework for a management system (Brodin, 2015a)	<ul style="list-style-type: none"> - Determines threats through a risk assessment. - Develop strategies or policies for the governance of BYOD. - Planning before policy. implementation. An evaluation of the strategy is conducted. 	<ul style="list-style-type: none"> - The role of compliance for the governance of BYOD is not considered. - Adoption in an SMME environment is not cited.
BYOD privacy & culture governance framework (Selviandro et al., 2015)	<ul style="list-style-type: none"> - Determines the culture of the organisation. - Provide a clear definition for the respective privacy concerns. - Develops a policy for the management of BYOD. 	<ul style="list-style-type: none"> - The employee role in the management of BYOD is not considered. - The SMME environment is not cited.

Enterprise and BYOD space BYOD Security Framework (Wang et al., 2014)	<ul style="list-style-type: none"> - States that the organisational context must be considered when managing BYOD. - There is a BYOD device analysis and IT Administration. - There is a BYOD policy in place. - Compliance is incorporated. 	<ul style="list-style-type: none"> - There is a lack of adequate risk management. - The SMME environment is not cited.
---	--	--

The critical evaluation of the existing BYOD frameworks represented in Table 5.3 provides evidence that they consist of some aspects that are relevant to use when formulating the contribution framework for this study. However, with some aspects identified to be relevant to this study, it is clear from the evaluation that none of the four existing BYOD frameworks specifically incorporates SMMEs. Seeing that none of the four existing BYOD frameworks specifically incorporates SMMEs, this study will develop a contribution framework that will incorporate the management of BYOD specifically in SMMEs.

Each of the four frameworks discussed will contribute in some aspect to the resultant contribution framework to be developed in this study. Additionally, it is important that the resultant contribution framework meet specific design principles. Furthermore, there are certain characteristics that BYOD frameworks are composed of that were identified during the literature review of the existing frameworks for BYOD. Therefore, it is important that the characteristics of BYOD be specified for the contribution framework to be developed.

Phase 2 states that the development of the artefact should be informed by design principles. There were also characteristics for BYOD identified during the literature review of the existing framework for BYOD. The design principles and characteristics for BYOD will form the basis for the initial draft of the contribution framework. Consequently, the next section discusses the principles and characteristics of the BYOD Management Framework.

5.4. Phase 2.2: Characteristics and principles of the BYOD Management Framework

In subsection 5.3.1, the literature review of some existing BYOD frameworks provides concise evidence that there is a need for some framework to assist in the management of BYOD in SMMEs. With this in mind, this study conducted a further literature review to identify the core aspects of such a framework to be developed. The foundation for the core aspects of the principles for the BYOD Management Framework and the information security characteristics of BYOD are discussed in the following subsections.

5.4.1. Principles of the BYOD Management Framework

The research approach discussed in Chapter 4, states that an artefact should be developed to address the real-life problem identified by the researcher. Furthermore, upon the completion of the development of the artefact, it must be validated against particular principles to determine the applicability of the artefact for the stakeholders. Consequently, this study formulated four principles that would be used to validate the artefact once it has been developed. The principles for a typical BYOD framework in SMMEs should cater for the following:

Scalability – The contribution should be scalable for an SMME environment.

Utility – The contribution should be usable in an SMME environment.

Efficacy – The contribution should be efficient and developed with the SMME environment in mind.

Quality – The contribution should be formulated to provide value in an SMME environment.

SMMEs consist of different sizes of enterprises that range from Survivalist enterprises to larger and well-established Medium enterprises. Consequently, the contribution framework must be scalable in order to accommodate the various sizes of the SMME enterprises. Therefore, the design principle of scalability is important.

An SMME will be limited by their size and financial stance in order to acquire and house the particular resources they need, for example basic ICT. As a result, an SMME will adopt BYOD within their organisations as it reduces the costs associated with the technology and also saves space required for the ICT. However, most SMMEs might be unaware of the

information security threats that could occur through the adoption of BYOD. Thus, the contribution framework must be usable by providing clear and useful information regarding the benefits and risks of BYOD, which could assist the SMMEs. Therefore, the design principle of utility is important.

SMMEs, like most large organisations, want to be constantly growing and be productive within their respective environments. The use of BYOD in SMMEs could allow SMMEs to be constantly productive, whilst growing from very small to medium enterprises. With this in mind, the contribution framework should be developed to permit SMMEs to be efficient and develop with the SMME environment in mind. Therefore, the design principle of efficacy is important.

Previously, in subsection 5.3.2., it was highlighted that the existing frameworks for BYOD do not incorporate SMMEs. However, some SMMEs are adopting BYOD in their organisations with no proper management associated. Consequently, the development of the contribution framework could assist SMMEs in their management of BYOD and in turn, this could provide value to them. Thus, the design principle of quality is important.

With these four principles for effective management of BYOD in SMMEs argued, an appropriate contribution towards the management of BYOD can be devised. However, before the formulation of the contribution framework, it is vital to consider the characteristics of BYOD that form the basis of the development of the framework.

5.4.2. Characteristics of BYOD

The literature on BYOD indicates that there are BYOD characteristics that should be formulated to form part of the basis for developing a framework. The BYOD characteristics in this research were devised by conducting a literature review of the characteristics of BYOD incorporated in the existing BYOD frameworks (section 5.3.), and other related literature on the characteristics of BYOD. Below is a list of eight BYOD characteristics identified from literature that an organisation should ideally follow:

BYOD Characteristics:

C1: There must be risk identification:

- “BYOD is an institutionalised security risk which small scale organisations need to assess and evaluate before blindly embracing the practice” (Madzima et al., 2014).
- “There are many potential risks and threats to confidential information resources and assets in organisations use BYOD devices” (Garba, Armarego, & Murray, 2015).

C2: There must be security requirements stipulated for BYOD:

- “The main goals of information security are confidentiality, integrity and availability” (Mir, Dar & Quadri, 2011).
- “Legal and liability issues should be considered and stated in the BYOD policy” (Yang, Vlas, Yang, & Vlas, 2013).

C3: The organisational context must be considered:

- “Uncontrolled environments present more dynamic risks within the specific context and circumstances of that environment” (Allam, Flowerday & Flowerday, 2014).
- “Organisations require accurate and reliable information because they communicate and manage substantial information resources” (Garba, Armarego, & Murray, 2015).

C4: There must be a BYOD device analysis:

- “BYOD consists of the use of personal devices. Only the definition does not state which devices it concerns” (Hensema, 2013).
- “Devices should be registered for participation in the BYOD programme, officially approved for use, and provisioned with required security settings” (Zahadat et al., 2015).

C5: The organisation must take into context the employee role:

- “Users of mobile devices need to be aware of threats the mobile device threats and have competent skills to secure their devices” (Harris, Patten, & Regan, 2013).
- “Users should be educated as they perform their daily activities, with frequent policy reminders that are non-intrusive and relevant to their current task” (Charbonneau, 2011).

C6: There must be IT Administration within the organisation:

- “Organisations should realise the impact BYOD can have on technical support” (Hensema, 2013).
- “It is crucial for organisations to employ a proper security model for mobile devices as security challenges will increase in organisations” (Eslahi Meisam & Var Naseri Maryam, 2014).

C7: There must be a BYOD policy:

- “Policies are good starting points for gaining control on an enterprise as they provide guidelines for BYOD adoption” (Madzima et al., 2014).
- “The policy should provide clarity on how devices will be used and how IT can meet those needs” (Dulaney & Debeasi, 2011).

C8: An organisation must have compliance:

- “A BYOD policy is likely to improve compliance by educating employees the risks associated with their devices” (Madzima et al., 2014). “Violation of the policy should have severe punishment” (Johnston, Warkentin, & Siponen, 2015).
- “Companies must re-evaluate BYOD compliance” (French, Guo, & Shim, 2014).

The eight characteristics for BYOD discussed in this subsection and the principles discussed in the previous subsection will form the basis for the initial draft of the contribution framework.

5.5. Phase 2.3.: The development of the BYOD Management Framework

The literature review and how it was used in this research allows the researcher to illustrate an initial draft of the theoretical framework. The initial draft of the framework will be developed and further refined through a cyclic process until it is satisfactory. Therefore, the following subsections will discuss the development of the initial draft of the theoretical framework.

5.5.1. Initial BYOD Management Framework

In the previous section, the eight characteristics and four principles that form the basis for the development of the theoretical framework were discussed. From the discussion of the characteristics and principles of BYOD, it was emphasised that the initial draft of the theoretical framework to be developed, should eventually meet the design principles and

BYOD characteristics defined in this research. Furthermore, the initial draft of the theoretical frameworks should incorporate some aspects analysed from the existing BYOD frameworks (Section 5.3.), that may be relevant to the theoretical framework. Thus, this study aimed to address the characteristics, principles and aspects of the existing BYOD frameworks to develop an initial draft of the theoretical framework which will be discussed in this subsection. A graphical representation of the initial draft of the theoretical framework can be viewed in Figure 5.5. As seen from the graphical representation, there are different aspects composed within the theoretical framework.

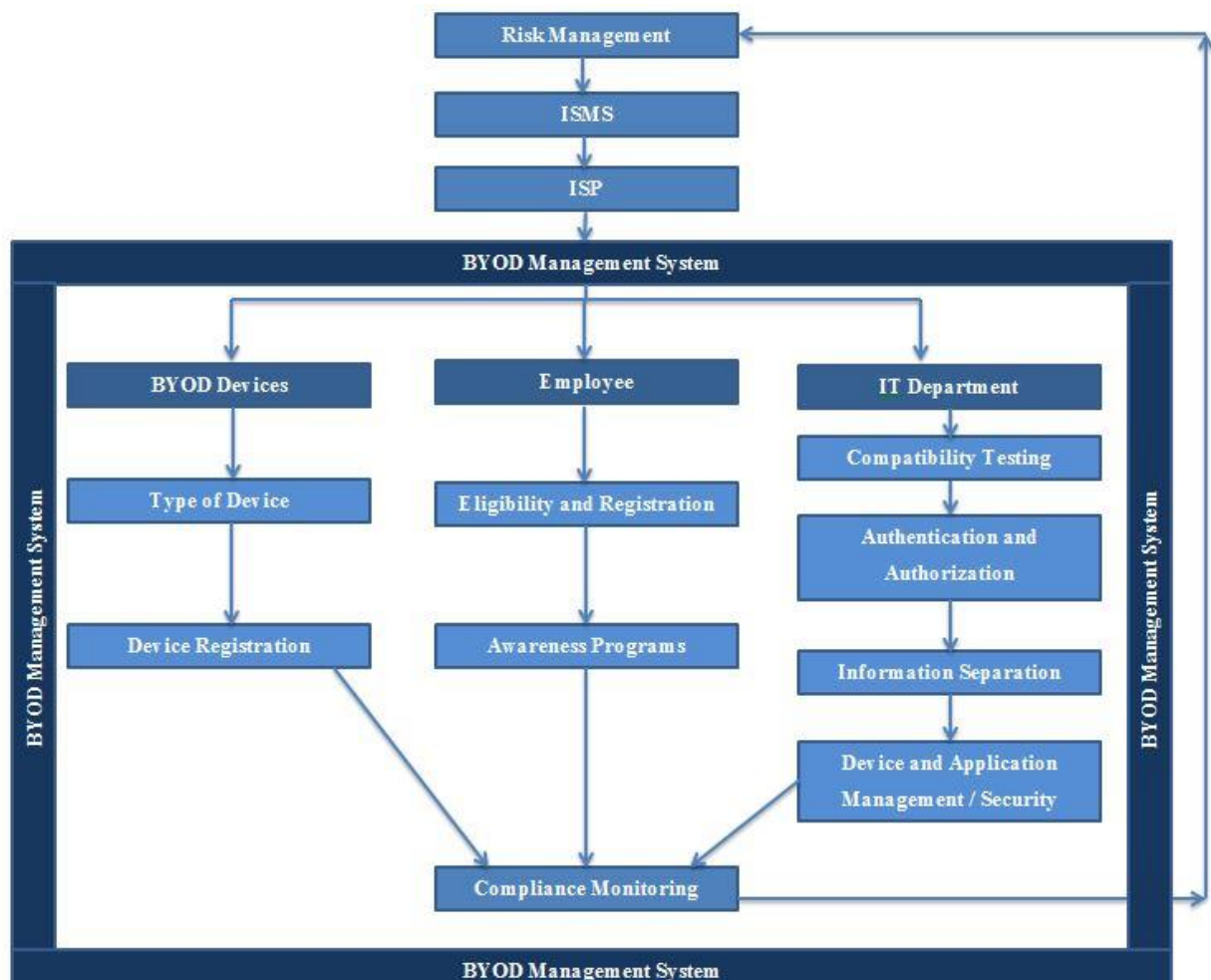


Figure 5.5: Initial draft of the theoretical framework (Noluvuyo Fani)

A brief description of each of the aspects contained within the theoretical framework is provided below.



Figure 5.6: The first aspects in the theoretical framework

In Figure 5.5, the aspect at the top is Risk Management. In Risk Management, the organisations should identify any risks and problems associated with BYOD that could affect their particular organisation. The two aspects leading from the Risk Management aspect represented in Figure 5.6, is the aspects of Information Security Management System (ISMS) and the Information Security Policy (ISP). In these two aspects, the legal regulatory issues that impact the use of BYOD in organisations should be identified once risk management has been implemented.

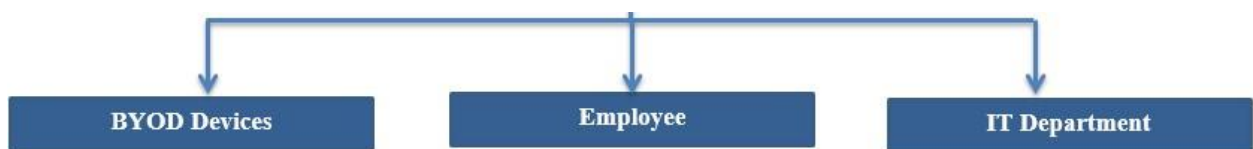


Figure 5.7 : The third aspects in the theoretical framework

Figure 5.7 represents the next level of aspects composed in the theoretical framework which consists of; the BYOD devices, Employee and IT Department. The aspects were formulated to highlight that organisations should develop and implement policies, controls, education and control measures towards the management of BYOD. These aspects are influenced by the completion of the implementation of the preceding aspects.

The last aspect to be discussed is Compliance Monitoring. This aspect addresses the monitoring of the developed framework to monitor whether the BYOD users comply with the systems in place for the management of BYOD, such as policies. Furthermore, when compliance is monitored and the employees do not comply with to the policy, actions can be taken against the employee. Thus, this aspect takes into regard any amendments that need to

be addressed regarding the management of BYOD. This can be conducted on a bi-annual or on a certain period of time stipulated by the organisation.

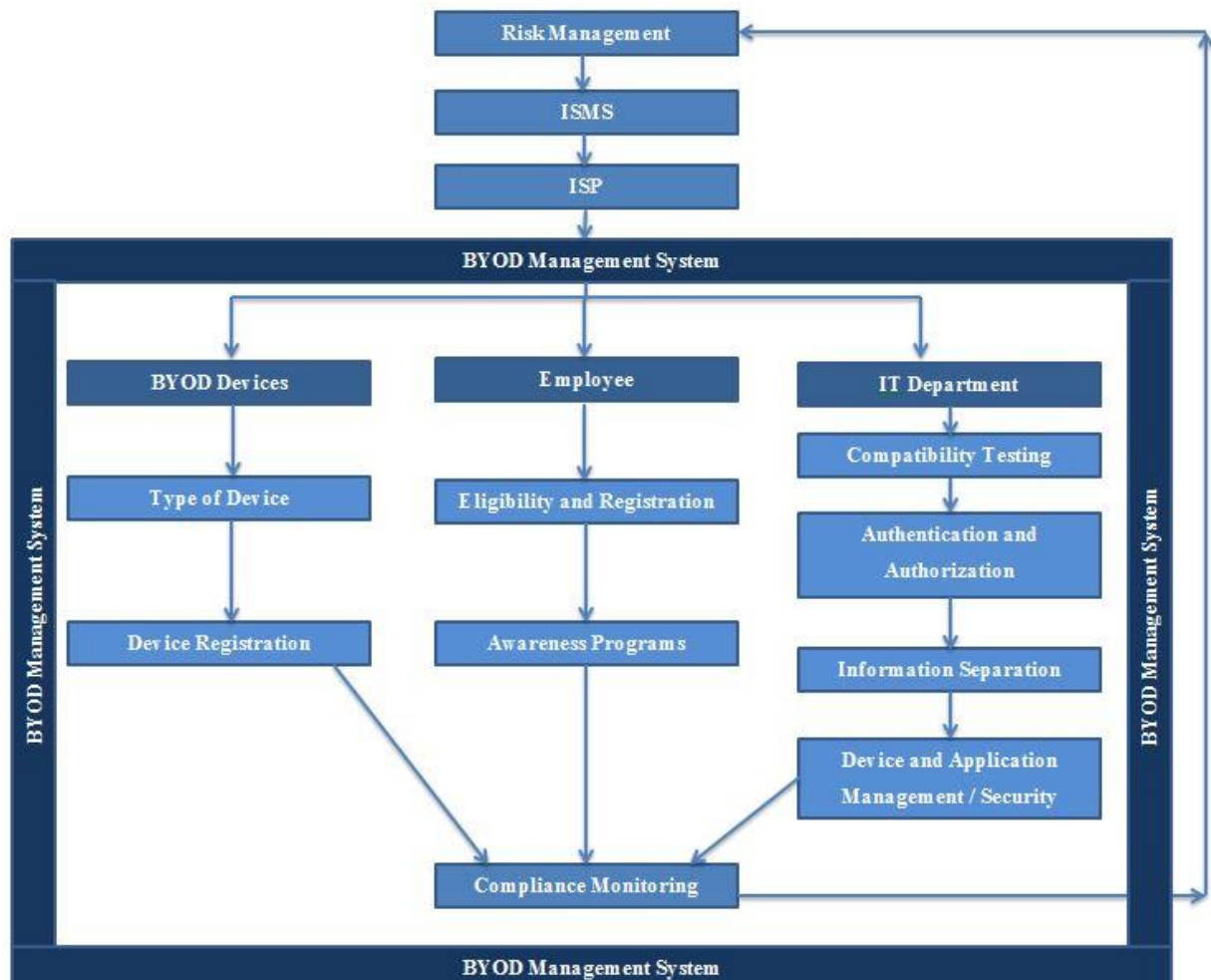


Figure 5.8: The theoretical framework for BYOD

Once the initial draft of the theoretical framework was established, it was refined through a cyclical process of iterations. Figure 5.8 illustrates the established theoretical framework before refinement. The process of refinement included engagement with the respective stakeholder which is discussed in the next section.

5.6. Phase 3: Process to the refinement of the BYOD Management Framework

Table 5.4: Phase 3 of the research process

Phases	Element	Position in research
Phase 3: Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteration)	
	Phase 3.1: Participants	Participants acting as stakeholders need to be identified.
	Phase 3.2: Data collection	Data will be collected from the stakeholders based on initial theoretical framework and intervention.
	Phase 3.3: Data analysis	This data is analysed and the intervention will be adapted according to the analysed data received from the stakeholder
	Phase 3.4: Implementation of intervention	
	Phase 3.5: (Second and further iterations)	Second and further iteration will be implemented, with data collection and analyses with the stakeholders, until the stakeholder is satisfied.

Phase 3, depicted in Table 5.4, states that participants acting as stakeholders need to be identified. The participants are used to collect data on the relevance of initial draft of the theoretical framework for SMMs. The data collected will be analysed and will assist in

amending towards finalising the artefact through iterative cycles of refinement until the stakeholder is satisfied. The practitioners (stakeholders) identified for this research study stemmed from local government (a typical example of an SMME), in particular, a District Municipality in the Western Cape region. The District Municipality is applicable to this study because it is currently adopting BYOD and the District Municipality meets criteria for an SMME.

5.6.1. Phase 3.1 - Phase 3.4: [Cycle 1] Data collection and analysis of the theoretical framework

In the previous subsection, the initial draft of the theoretical framework was developed and presented. Additionally, participants acting as stakeholders were identified and data collected from the stakeholders assists in the formulation of the initial draft of the theoretical framework. Nonetheless, with the initial draft of the theoretical framework developed, the researcher scheduled a visit with the stakeholder. The visit to the stakeholders was used to conduct data collection on the opinions of the participants on the appropriateness of the initial draft of the theoretical framework. The visit was scheduled for 19 August 2015 at 09:00 am, at the District Municipality. The participants in the session, were various ICT, auditing and risk management professionals who would form part of the BYOD management team in their particular SMME. The session lasted approximately an hour.

During the visit to the stakeholder, the researcher presented the problem identified and the initial draft of the theoretical framework to the stakeholders. The stakeholders made inquiries on the problem and the various aspects the theoretical framework where it was relevant.

The researcher analysed the responses of the stakeholders regarding the problem and theoretical framework presented during the visit to the stakeholder. Feedback from the stakeholders indicated that there is currently a lack of BYOD management in their particular SMME environment. Furthermore, employee's access, communicate, process and store organisational information on their mobile devices with no proper security mechanisms, such as antivirus software, in place. Consequently, feedback from the stakeholders provides evidence that the problem of the risks associated with BYOD, identified by the researcher, and is a real-life problem experienced by SMMEs. Therefore, there is indeed a need to

develop a BYOD Management Framework to assist SMMEs to management their BYOD environment.

The stakeholder indicated that they required assistance in the management of BYOD and the initial draft of the theoretical framework was applicable in their SMME. With interest shown by the stakeholder on the particular research problem, refinement of the framework could start.

5.6.2. Phase 3.5.: [Cycle 2] Refinement of the theoretical framework (mind map)

The refinement of the initial draft theoretical framework was to conduct a literature review to determine whether the aspects currently within the theoretical framework are sufficient. When the aspects that are sufficient for the contribution framework are identified, the theoretical framework can be refined. There are different aspects derived in literature for a framework and a mind map was used to illustrate the various aspects contained in various BYOD frameworks. A mind map is used when there is a need to outline the main idea with different concepts linked it. In this instance, BYOD is the “main idea” and the various aspects that can be composed in frameworks are the “different concepts”. The graphical representation of part of the mind map can be seen in Figure 5.9, with the complete mind map attached as Appendix A. In Figure 5.9, some of the aspects that would be relevant to use in the development of the contribution framework are illustrated. Previously, in Section 5.3, there were four existing BYOD frameworks that were analysed and evaluated to determine their applicability in SMMEs for the management of BYOD. The evaluation indicated that the existing BYOD frameworks lack in addressing the management of BYOD SMMEs. Therefore, the mind map was used to determine what can be sourced from the existing BYOD frameworks that could be used in the management of BYOD framework for SMMEs.

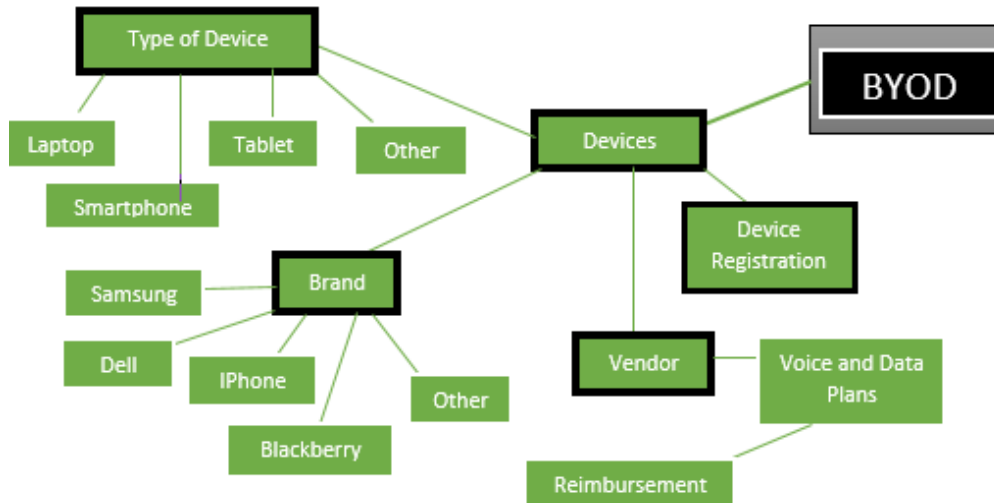


Figure 5.9: Partial representation of the mind map

Once the mind map was drafted, a focus group was scheduled to substantiate the aspects the mind map.

5.6.3. Phase 3.5.: [Cycle 3] Refinement of the theoretical framework (focus group)

A focus group consists of a group of individuals who provide their knowledge on a specific topic. The concept of the focus group in this study was to substantiate the aspects identified in the mind map discussed above, as being applicable to be used in the refinement of the theoretical framework. The focus group was scheduled for 23 October 2015 at an accomplished university in the Eastern Cape region. A group of four ICT Masters Students who had an idea of BYOD, participated in the focus group session. The opinions of the participants on the aspects to be included in the development of the contribution framework were recorded and were used to refine the theoretical framework.

Upon the completion of the focus group, the theoretical framework was refined. Figure 5.10 depicts the refined theoretical framework. In the illustration below, it can be seen that there is the addition of a BYOD Policy Plan at the bottom of the framework, which was not present in the initial draft of the theoretical framework discussed earlier (Figure 5.5). The BYOD Policy Plan will address the development and management of the BYOD policy.

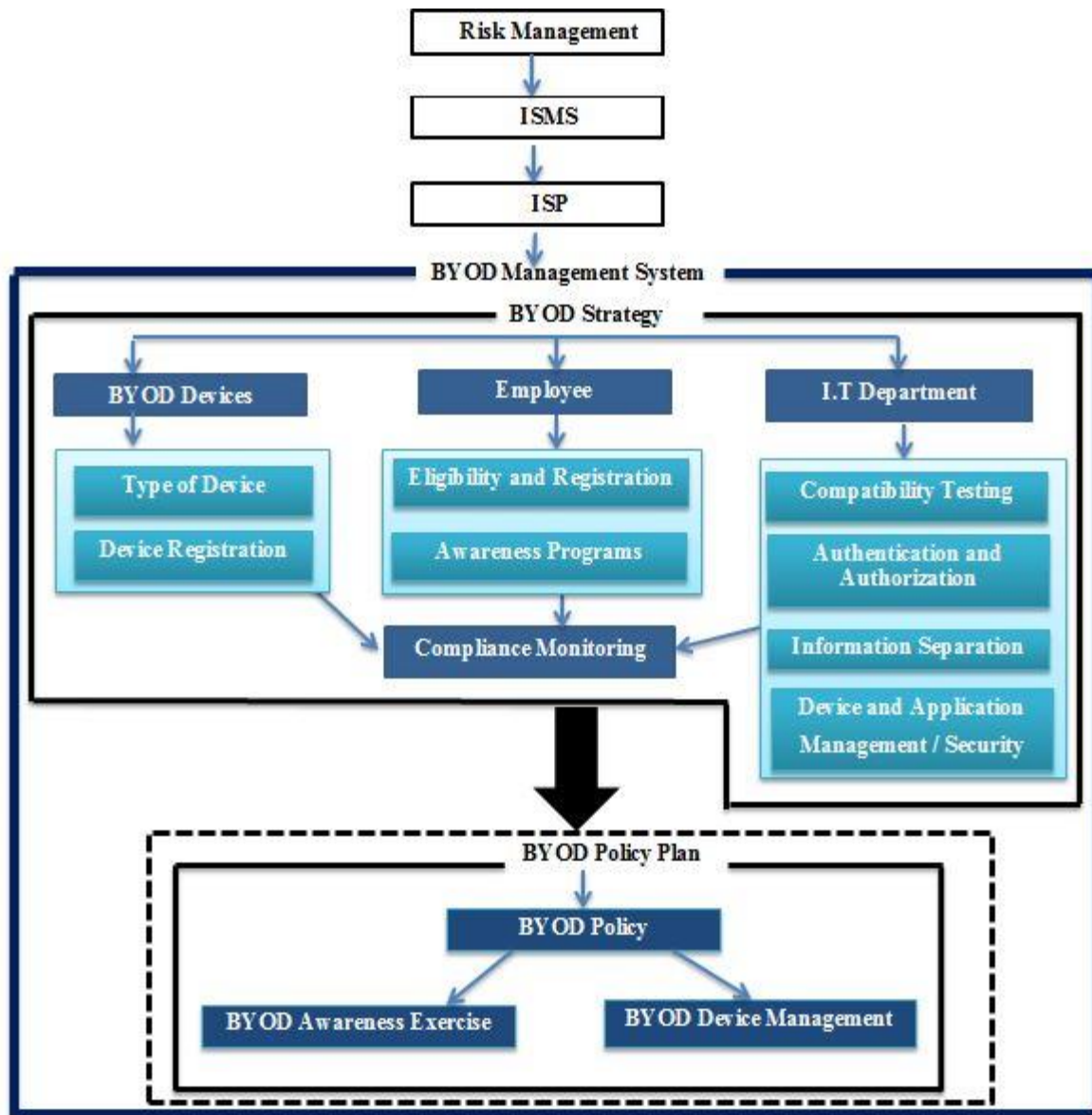


Figure 5.10: Refined theoretical framework

Leading the refinement of the theoretical framework, a survey in the form of a questionnaire was developed. The questionnaire was used in this study to determine the applicability of the refined theoretical framework to the stakeholder environment. This was done in Cycle 4.

5.6.4. Cycle 4: Refinement of the theoretical framework (questionnaire and semi-structured interviews)

The questionnaire was constructed on an Excel spreadsheet and divided into the three aspects: Devices, Employees and IT services. Responses to the questionnaire were made by ICT representatives from a District Municipality in the Western Cape region. The representatives

indicate on the questionnaire, the statement they agree to. The representative's feedback on the questionnaire assists in determining whether the theoretical framework developed thus far, is sufficient to be used in their SMME environment. Figure 5.11 provides a representation of the questionnaire questions formulated (refer to Appendix B for more questions).

Bring Your Own Device (BYOD) / Bring Your Own Municipal Device (BYOMD) The purpose of this questionnaire is to determine the municipal requirements for BYOD. Please answer the questionnaire by choosing from the dropdown list in the <u>Answer</u> column or by providing an details in the <u>Comment</u> column.		
Question	Answer	Justification
1. Devices		
1.1.) Type of Devices:		
1.1.1.) Which type of mobile devices are currently used within the municipality?	<input type="radio"/> Laptop <input type="radio"/> Smartphone <input type="radio"/> Tablet <input type="radio"/> All of the above <input type="radio"/> Other	
1.2. Device Registration:		
1.2.1.) Which type of brands are currently used for mobile devices?	<input type="radio"/> Samsung <input type="radio"/> Blackberry <input type="radio"/> Nokia <input type="radio"/> iPhone <input type="radio"/> Other	
1.2.2.) Who is currently responsible for authorizing users who recieve the mobile device?	<input type="radio"/> I.T Department <input type="radio"/> Manager <input type="radio"/> Supervisor <input type="radio"/> Employee <input type="radio"/> Other	
1.2.3.) Who is responsible for registering the mobile devices?	<input type="radio"/> I.T Department <input type="radio"/> I.T Technician <input type="radio"/> Any I.T employee <input type="radio"/> Other	
1.3.) Vendor:		
1.3.1.) Who is the current vendor for data and voice services? Please provide details in the justification column		
1.3.2.) Does the municipality allow employees to make use of their own personal mobile devices to complete business tasks?	<input type="radio"/> Yes <input type="radio"/> No	
data costs?	<input type="radio"/> Yes <input type="radio"/> No	

Figure 5.11: Sample questionnaire questions

Once the questionnaire was completed, a second visit with the same stakeholders was scheduled on 17 August 2015. However, an expert in ICT and Risk Management, specifically, a Senior Officer for ICT systems and a Risk and Logistics Administrator were the identified representatives in this instance. Formal semi-structured interviews were conducted and during the interviews, the questionnaire was presented to the representatives. The semi-structured interview lasted approximately an hour and results from the session allow the researcher to conduct the final cycle of refinement to the theoretical framework.

Nonetheless, a mixed-method approach (mind map, focus group and questionnaire) derived from the research approach used in this study was used to assist in the refinement of the theoretical framework. The mixed-methods (mind map, focus group and questionnaire) used to refine the theoretical framework are represented in a process model in Figure 5.12.

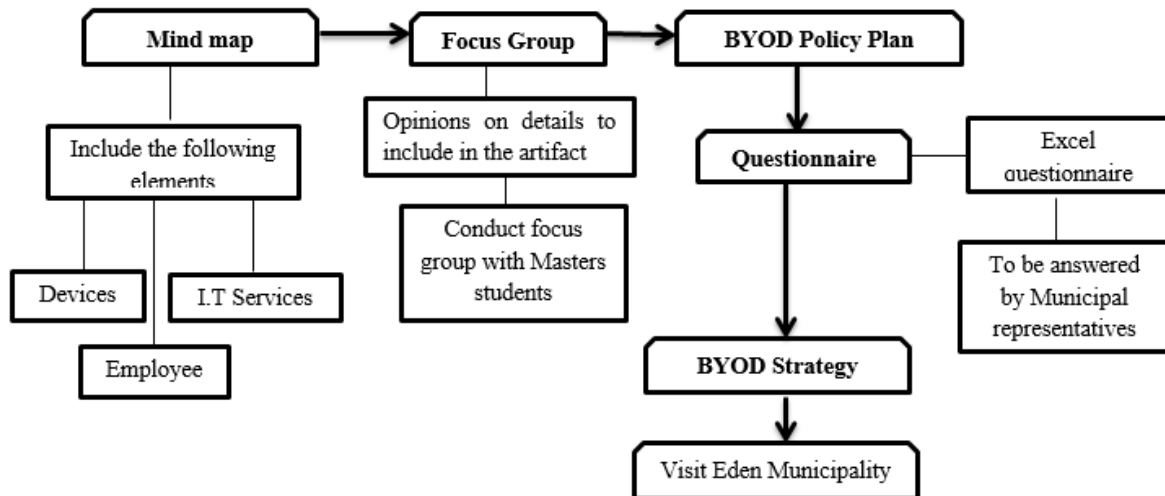


Figure 5.12: The process model of the cycles of refinement

As seen from the process model above, all the cycles of refinement for the theoretical framework is modelled. A mixed-method approach (mind map, focus group and questionnaire) derived from the research approach used in this study was used to assist in the refinement of the theoretical framework. The refinement of the theoretical framework has resulted in a final contribution framework (BYOD Management Framework). Consequently, the BYOD Management framework developed will be further discussed in the next section.

5.7. BYOD Management Framework

In the previous section, the initial draft of the theoretical framework was refined through a cyclic process and the outcome was the formulation of the BYOD Management Framework. The BYOD Management Framework is divided into six sections; the BYOD Security Requirements, BYOD Security Management, BYOD Strategy and the BYOD Policy Plan, BYOD Policy Implementation and BYOD Compliance. Figure 5.13 illustrates the BYOD Management Framework.

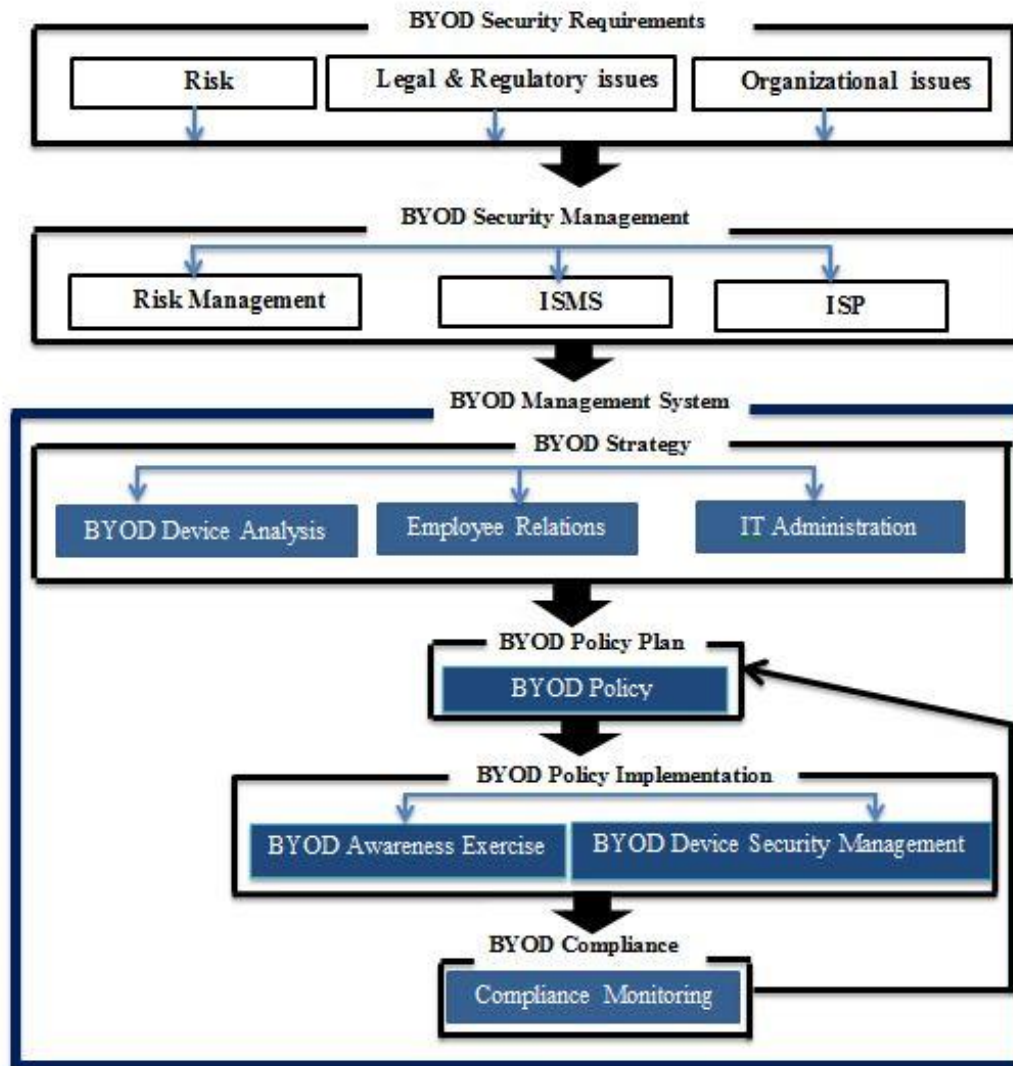


Figure 5.13: BYOD Management Framework

A narrative of the six sections of the finalised BYOD Management Framework is provided below.

Section 1:

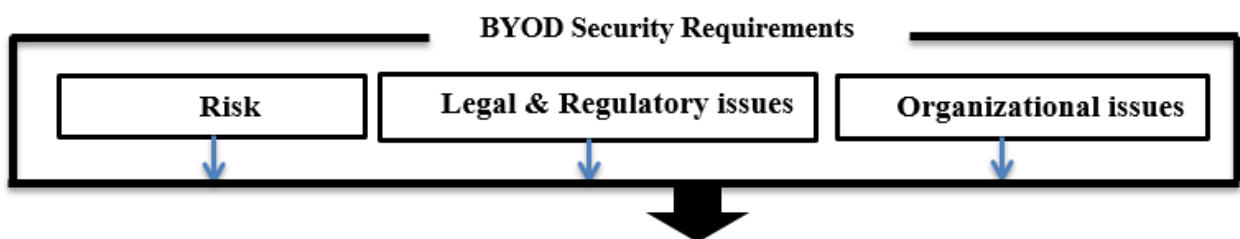


Figure 5.14: BYOD Security Requirements

The top section in the framework titled BYOD Security Requirements, displayed in Figure 5.14 and addresses issues related to the risks to the CIA of organisational information when an organisation implements BYOD. Furthermore, the legal and regulatory issues relating to BYOD and other security requirements for the organisation are identified. A description of the aspects contained in BYOD Security Requirements are:

- **BYOD Security Requirements:**
 - **Risk:** Determine risks to the CIA of the organisational information
 - **Legal and Regulatory issues:** Identify any legal and regulatory issues that could influence the adoption of BYOD
 - **Organisational issues:** Identify other security requirements for the organisation

Section 2:

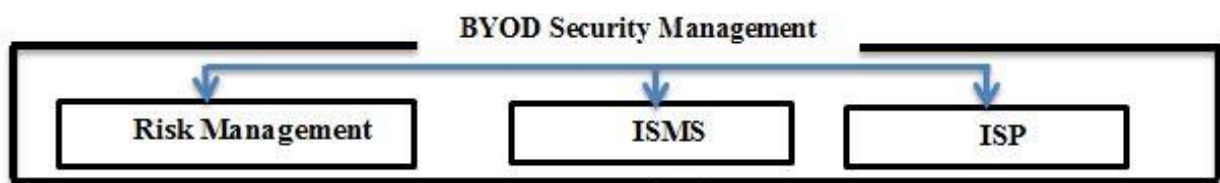


Figure 5.15: BYOD Security Management

The next section below BYOD Security Requirements (presented in Figure 5.14) is BYOD Risk Management. Figure 5.15 displays the aspects of Risk Management, ISMS and Information Security Policy (ISP) contained in BYOD Security Management. The purpose of BYOD Security Management is to determine how the risks associated with BYOD and the security risks that were identified in the BYOD Security Requirements (Figure 5.14) can affect the way BYOD Security Management (BYOD users in the organisation) implement BYOD. Below is a description of the aspects contained in BYOD Security Management:

- **BYOD Security Management:**
 - **Risk Management:** Identify the risks associated with BYOD
 - **ISMS:** Protect the organisational information from any risks identified with BYOD
 - **ISP:** Determine what the ISP states about information security

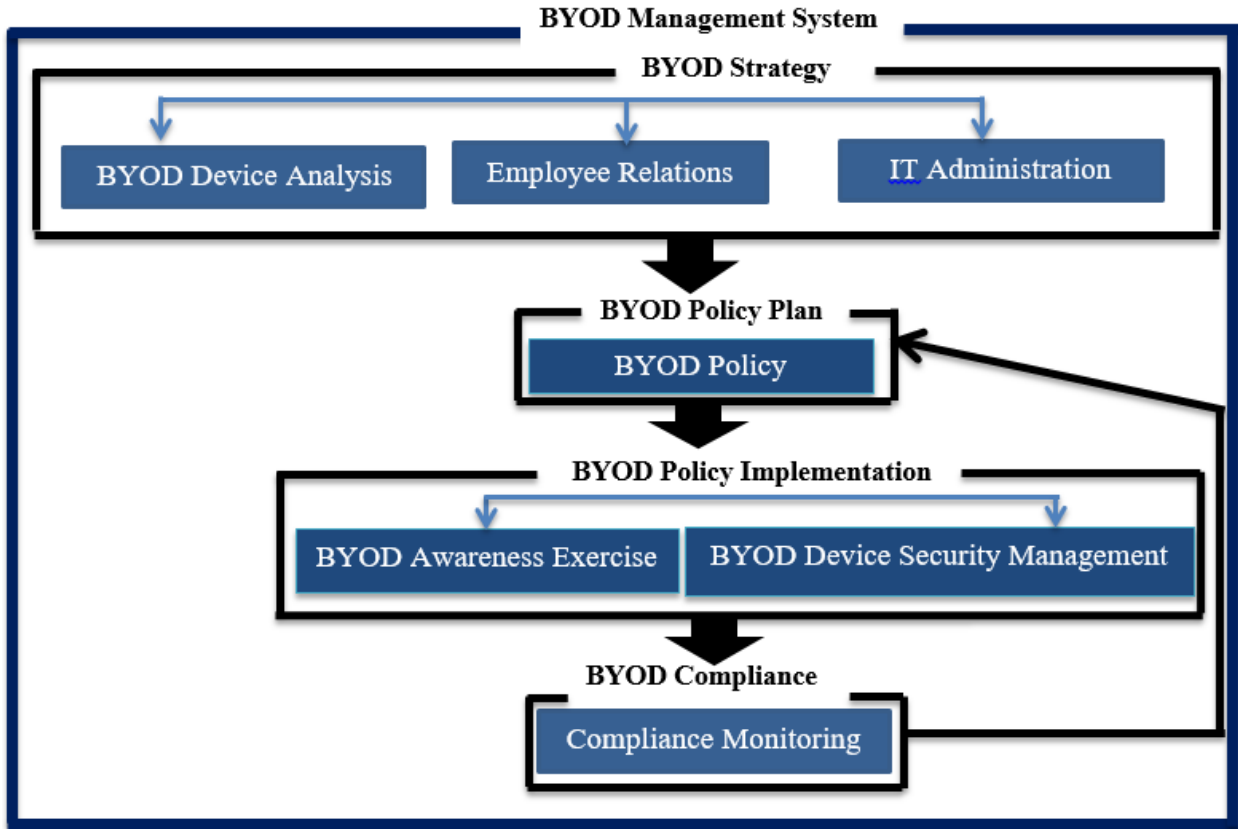


Figure 5.16: BYOD Management System

The third section to the sixth section is integrated in the BYOD Management System, which can be viewed in Figure 5.16. In these aspects, the decisions on the strategy for how BYOD will be managed are conducted. A discussion of the third section to the sixth sections is provided below.

Section 3:

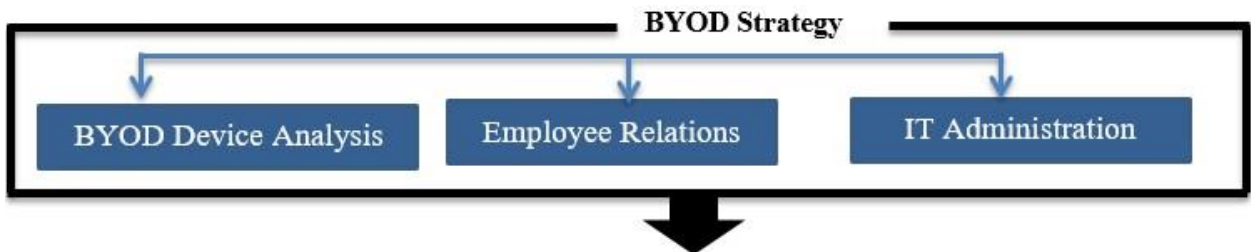


Figure 5.17: BYOD Strategy

The third section in the BYOD Management Framework is the BYOD Strategy. The BYOD Strategy represented in Figure 5.17 relates to the decision-making process of the management BYOD by taking into account the aspects of BYOD Devices, Employee Relations and IT Administration. This includes decisions on the type of mobile devices to be incorporated with the adoption of BYOD and the eligible employees who will be the BYOD users, amongst others. The aspects in the BYOD Strategy are divided as follows:

- **BYOD Strategy:**

BYOD Devices:

- **Type of device:** Determine the type of device/s to be incorporated into the SMME environment for BYOD.
- **Device registration:** The preferred devices should be registered within the organisation so that they can be identified and be provided with rights to access sensitive organisational information.

Employee Relations:

- **Eligibility and Registration:** The organisation must determine the eligible employees that will be BYOD users and there should be registration of the eligible employees.
- **Awareness Programmes:** The organisation should determine appropriate awareness programmes.

IT Administration:

- **Compatibility testing:** The BYOD devices require compatibility testing.
- **Authentication and Authorisation:** BYOD users need to be authenticated and authorised.
- **Information separation:** Information should be separated into personal and organisational information on the BYOD device.
- **Device and Application Management / Security:** The information and applications within the BYOD device require constant protection.

Section 4:



Figure 5.18: BYOD Policy Plan

Once the decisions on the BYOD Strategy are concluded, the fourth section, a BYOD Policy Plan will commence. The BYOD policy should stipulate how the organisation will manage BYOD. Within this research study, a literature review was conducted on the various BYOD policies currently in place and a draft BYOD policy was developed (Appendix D). The developed draft BYOD policy stipulates important aspects for the overall management of BYOD. The important aspects are inclusive of the scope of users that the policy to and the type of mobile devices that can be used for BYOD. Stipulating important aspects in the draft BYOD policy allows the organisation to implement BYOD with a control in place. Figure 5.18 displays the fourth section, which is inclusive of the following aspects:

- **BYOD Policy Plan:**
 - **BYOD Policy:** A BYOD policy should be a documented guideline for the management of BYOD.

Section 5:

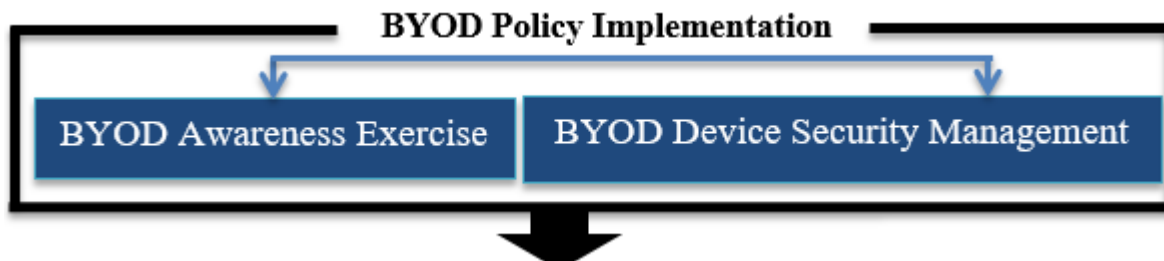


Figure 5.19: BYOD Policy Implementation

When the BYOD Policy is developed, it can be distributed amongst the employees of the organisation and implemented or enforced. The implementation of the BYOD policy will be supported by education, awareness exercises and aspects of BYOD Device Security Management. The implementation of the BYOD policy is addressed in the fifth section

namely, BYOD Policy Implementation, which can be viewed in Figure 5.19 and will be fulfilled according to the below statements:

- **BYOD Implementation:**
 - **BYOD Awareness Exercise:** This aspect will consist of the educational, awareness and training aspects of BYOD.
 - **BYOD Device Management:** BYOD device management will be addressed in this aspect.

Section 6:



Figure 5.20: BYOD Compliance

The sixth section displayed in Figure 5.20, is BYOD Compliance and relates to monitoring of the compliance with the BYOD policy. The aspect of Compliance Monitoring, in BYOD Compliance, is described below:

- **BYOD Compliance:**
 - **Compliance Monitoring:** There needs to be constant monitoring of compliance for BYOD.

The contribution of this research, namely, the BYOD Management Framework was discussed in this section. The BYOD Management Framework was developed with the assistance of the four existing BYOD frameworks (section 5.2.), four principles (subsection 5.3.1.) and eight BYOD characteristics (subsection 5.3.2.) in mind. Each of the existing BYOD frameworks discussed previously contributes in some aspect in the aspects composed in the resultant BYOD Management Framework developed in this study. Furthermore, the BYOD Management Framework adheres to the design principles and BYOD characteristics in that it incorporates all the aspects defined in them, when implementing the management of BYOD in SMMEs.

5.8. Conclusion

In this chapter, the execution of the three phases specified in the research process was emphasised. The first phase discussed the identification of the research problem, stakeholders and research objectives. The second phase discussed the process to the initial draft of the theoretical framework and the third phase discussed the iterative cycles of the refinement of the artefact.

The last phase of the research process, phase 4, consists of the process of artefact validation. The next chapter discusses the validation of the BYOD Management Framework.

Chapter 6: Validation of the BYOD Management Framework:

6.1. Introduction

From the previous chapter, it is clear how the BYOD Management Framework was developed and what it consists of. It was emphasised that stakeholders from local government assisted the researcher with the development and the refinement of the BYOD Management Framework. As a result, the finalised BYOD Management Framework was produced which consisted of six interrelated sections dedicated to the management of BYOD in SMMEs. With the finalised BYOD Management Framework at hand, it is important to complete the previously defined research approach. In order to do so, the BYOD Management Framework is validated.

Chapter 4 highlighted the four phases comprising the research approach. The first three phases have been discussed in the previous chapter. The first three phases were used to develop the BYOD Management Framework. Nonetheless, the fourth and final phase should still be addressed. Therefore, this chapter will discuss the validation process depicted in Figure 6.1 used to validate whether the BYOD Management Framework conforms to the four principles of scalability, utility, efficacy, and quality.

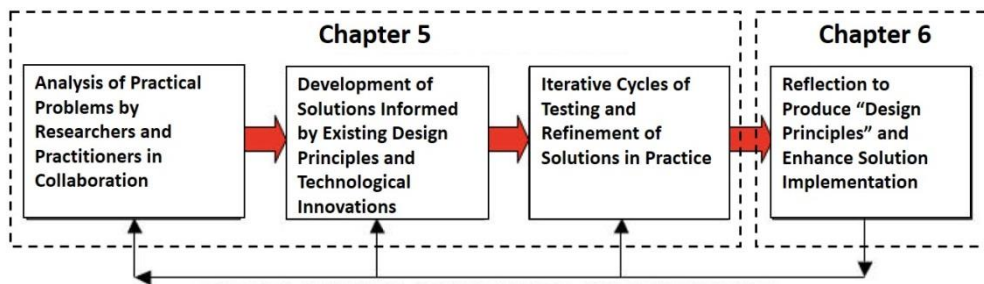


Figure 6.1: Four phases of the research process

To validate conformance to these four principles, this chapter will start by discussing the method used to analyse the data, which led to various results. Subsequently, the chapter will conclude with findings on the ability of the BYOD Management Framework to conform to the four principles of scalability, utility, efficacy, and quality.

6.2. Data Collection

To validate the BYOD Management Framework a workshop was conducted. This workshop was conducted over a period of two days, the 25th and 26th of April 2016. A total of 24

representatives from various Local and District Municipalities in the Eastern Cape region of South Africa attended the workshop. The representatives were inclusive of but not limited to experts in fields of ICT, internal auditing and risk, amongst others. It is important to note that these representatives are relevant to this study, as they would be most likely be appointed to assist their respective SMME environment with the management of BYOD. This is evident in that the representatives fall under the category B and C of local government, which are classified as having limited resources and finances (refer to subsection 1.5).

With regards to the design of the workshop, the two days dedicated to the workshop was divided into two sessions. The first session provided an explanation of the background and related problems associated with the implementation of BYOD in SMMEs. In essence, this provided the representatives with an understanding of BYOD and how it relates to an SMME or local government in this case. After establishing the link between local government and BYOD, the second session presented the BYOD Management Framework and its relevant aspects. During this session, a supporting document was provided to each of the representatives. This supporting document is a draft of a generic BYOD policy. This generic BYOD policy resembles an example of how a typical BYOD policy could look for any given SMME.

Figure 6.2 provides an extract of this draft BYOD policy, however, the entire BYOD policy can be seen in Appendix D. During the second session, the BYOD policy was used as a means to provide the representatives with a guide on how a policy for BYOD could look. In order for the representatives to develop a tailor-made BYOD policy, various statements contained within the BYOD policy were amended to suit the requirements of the particular SMME environment, or in this case the municipal environment. After amending the generic BYOD policy, a tailor-made BYOD policy was produced which concluded the second session.

1.3 Device Registration:

1.3.1. Authorized mobile devices to be used for BYOD must be registered.

1.4 Vendor:

1.4.1. The municipality will be responsible for acquiring mobile devices that are not personally owned by BYOD users.

1.4.2. Users with personally owned devices will be responsible for purchasing their mobile device. 1.4.3. Voice and data plans and costs will be acquired for users who meet the following requirements:

- Use your mobile device mostly outside the municipal offices.
- Users frequently travelling within the country, or overseas.
- Users who need frequently require access to the municipal information anywhere, anytime.

2. Employee Relations:

2.1 Eligibility:

2.1.1. Employees are divided into three different levels; Strategic level, Tactical level and Operational level. Therefore, eligible users for BYOD will be categorized by these levels. Criteria that determine who is eligible to make use of BYOD is:

- Job title
- Job function
- Location

Figure 6.2: Extracted an example of the BYOD policy

Upon completion of the two workshop sessions, a survey in the form of a questionnaire was conducted amongst the 24 representatives. The questionnaire was used to validate the ability of the BYOD Management Framework to conform to the four principles of; scalability, utility, efficacy and quality. Regarding the design of the questionnaire, the researcher made five statements. Each representative would then have to indicate on a Likert scale whether they 'strongly disagree', 'disagree', 'agree' or 'strongly agree' with the particular statement. Figure 6.3 provides a sample of the first two statements in the questionnaire. The complete questionnaire is attached in Appendix C.









1. The BYOD Management Framework is appropriate in local and district municipality environment regardless of their size.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
2. The different components of the BYOD Management Framework are clear and logical.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 

Figure 6.3: Extracted an example of the validation questionnaire

Furthermore, the questionnaire presented the representatives with three further open-ended questions. These open-ended questions aimed to determine whether there was anything lacking from the BYOD Management Framework, whether anything could be improved, and lastly if there was anything that stood out. By completing the questionnaire, the applicability of the developed BYOD Management Framework was validated. Additionally, the responses of the representatives indicated whether the BYOD Management Framework adheres to the four principles of; scalability, utility, efficacy, and quality. Table 6.1 represents the mapping of the four principles (as discussed extensively in subsection 5.4.1) with the five statements from the questionnaire.

Table 6.1: Workshop Questionnaire Structure

Principles	Statement no.	Description of statement
Scalability	1	The BYOD Management Framework is appropriate in local and district municipal environments regardless of their size.
Utility	2	The different aspects of the BYOD Management Framework are clear and logical.
	3	The BYOD Management Framework is well organised to be incorporated by the different levels of management (Top management, Middle management, Low level management) within the organisation.

Efficacy	4	The BYOD Management Framework is comprehensive in its inclusion of devices, employees, security, awareness and management of BYOD.
Quality	5	The BYOD Management Framework is useful in assisting local and district municipal environments with the management of BYOD.

After the representatives completed the questionnaire, the responses were collected in order to do an analysis thereof. The results stemming from the analysis aim to show that the BYOD Management Framework conforms to the four principles.

6.3. Data analysis and results

Taking into consideration the responses from the questionnaire, the outcome of each principle is discussed individually. The first result focuses on the conformance to the principle of scalability.

6.3.1. Results on the Principle of Scalability

As discussed in subsection 5.4.1, the principle of scalability aims to enable the developed BYOD Management Framework to be scalable to fit various sizes of SMME environments. With this in mind, the results of the feedback on the principle of scalability are represented in Figure 6.4.

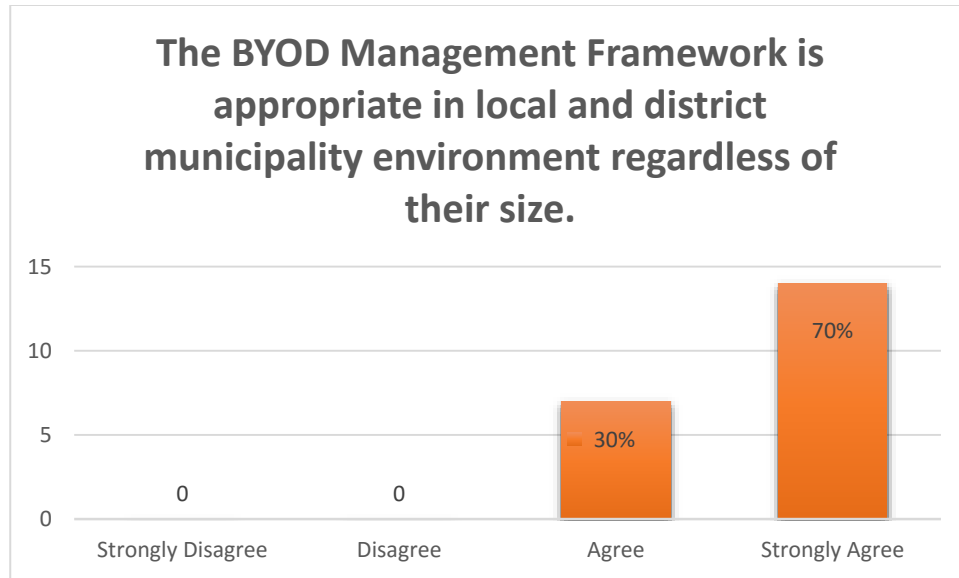


Figure 6.4: Results on the Principle of Scalability

In response to whether the BYOD Management Framework is scalable, 30% agreed, and 70% of the representatives strongly agreed that the BYOD Management Framework could be used in SMMEs, regardless of the size. Thus, it can be deemed that all the representatives agree that the BYOD Management Framework adheres to the principle of scalability.

6.3.2. Results on the Principle of Utility

Concerning the principle of utility, it is important to determine whether the BYOD Management Framework is practically usable in various SMME environments (as discussed in subsection 5.4.1). As seen in Table 6.1, two statements (3 and 4) were used to validate the principle of utility and the results of the two statements are presented in Figure 6.5 and Figure 6.6 respectively.

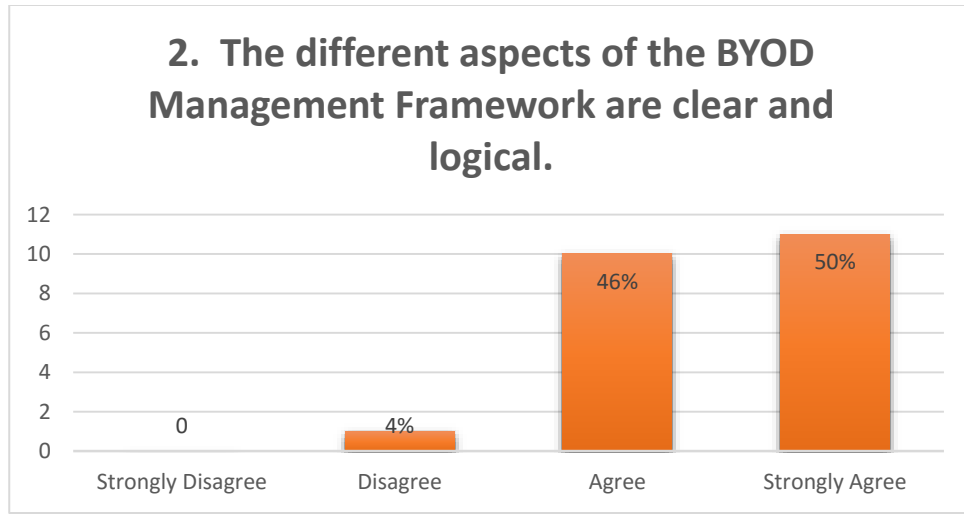


Figure 6.5: Results on the Principle of Utility

As seen in Figure 6.5, the first statement of the principle of utility was presented to the representatives. Of the 24 representatives, 50% strongly agreed that the BYOD Management Framework can be used in SMMEs. Furthermore, an additional 46% of the representatives agreed on the utility of the framework and 4% of the representatives disagreed. The fact that one of the representatives disagreed is most likely due to some of the representatives stemming from functions such as internal auditing amongst others. As a result, these representatives might not be too familiar with certain aspects of ICT.

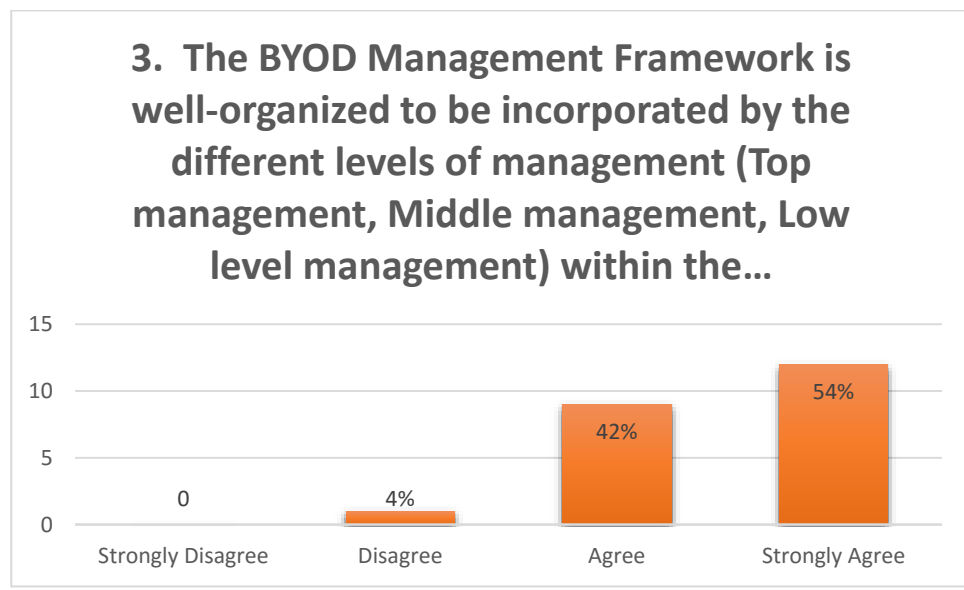


Figure 6.6: Second Set of Results on the principle utility

Figure 6.6 provides evidence that 54% of the representatives strongly agreed to the second statement. In doing so, the representatives strongly agreed that the BYOD Management Framework can be used in SMMEs. Furthermore, an additional 42% of the representatives agreed on the utility of the framework and 4% (one) of the representatives disagreed. Once again, this is most probably due to the fact that some of the representatives stemmed from another function, such as internal auditing, and not being too familiar with ICT. Nonetheless, the majority of the representatives agree with the fact that the BYOD Management Framework included the principle of utility satisfactorily. Thus, it can be concluded that the BYOD Management Framework adheres to the principle of utility.

6.3.3. Results on the Principle of Efficacy

The principle of efficacy was utilised to determine the efficacy of the BYOD Management Framework as per discussion in subsection 5.4.1. Figure 6.7 illustrates the results of the feedback on the principle of efficacy.

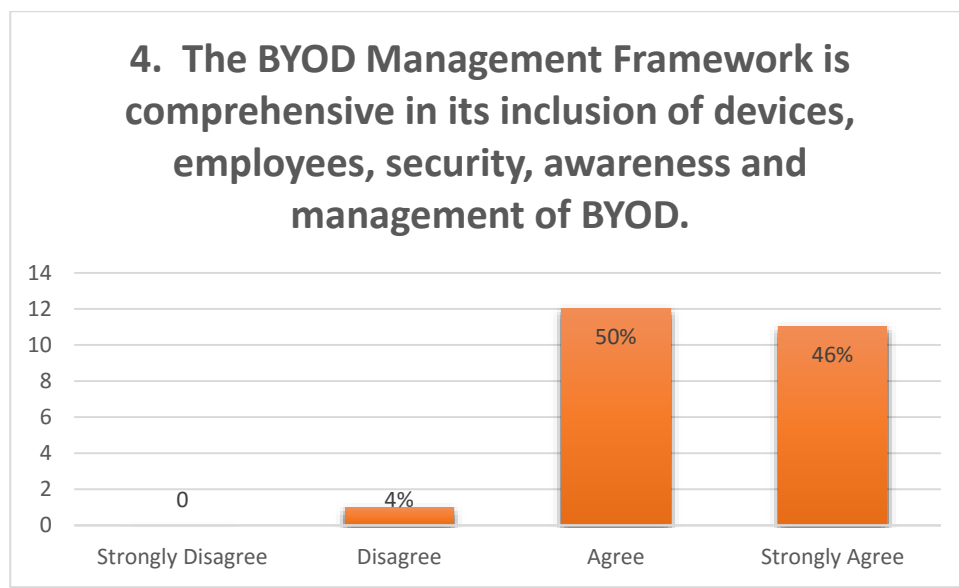


Figure 6.7: Results on the Principle of Efficacy

As seen in Figure 6.7, 46% of the representatives strongly agreed, 56% agreed and 4% of the representatives disagreed on the efficacy of the framework. The disagreement on the efficacy of the BYOD Management Framework could again be due to some of the representatives stemming from other functions that are unfamiliar with ICT, such as internal auditing and

risk. Nonetheless, the majority of representatives agreed with the incorporation of the principle of efficacy in the BYOD Management Framework.

6.3.4. Results on the Principle of Quality

As per subsection 5.4.1, the principle of quality aims to determine what the value of the BYOD Management Framework is for SMMEs. Figure 6.8 illustrates the results on the principle of quality.

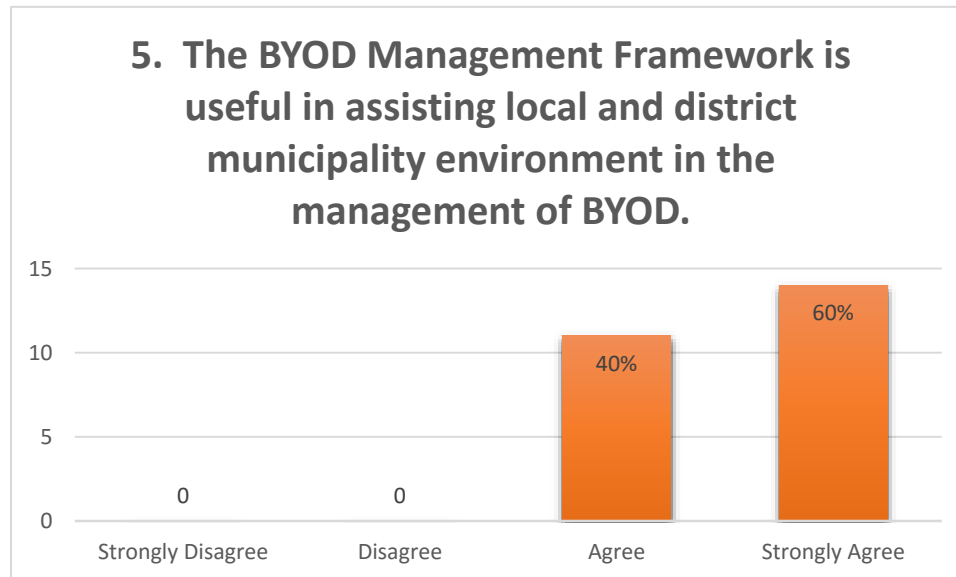


Figure 6.8: Results on the Principle of Quality

Figure 6.8 provides evidence that 60% of the representatives strongly agreed and 40% agreed that the BYOD Management Framework provides quality to SMMEs. Thus, it can be deemed that all the representatives agreed that the BYOD Management Framework adheres to the principle of quality.

Taking the aforementioned into account, it is important to provide the findings based on the conformance to the four principles of scalability, utility, efficacy and quality.

6.4. Findings

The questionnaire presented various statements that allowed for the successful validation of the BYOD Management Framework. This was done by validating the conformance of the BYOD Management Frameworks to the principles of scalability, utility, efficacy, and quality. With this in mind, the responses indicate that the representatives strongly agree that the

BYOD Management Framework is scalable to fit any sized SMME. Accordingly, the representatives agree that the BYOD Management Framework is usable and efficient within an SMME context as well as a municipal context. Furthermore, the majority of representatives agreed that the BYOD Management Framework will provide value to their municipalities. Only a small percentage of the representatives disagreed in this regard. The majority of the responses of the survey were overwhelmingly positive in nature. Table 6.2 tabulates the combined feedback from the representatives. Subsequently, Table 6.2 provides evidence that the representatives agree that the BYOD Management Framework conforms to the four principles of scalability, utility, efficacy, and quality.

Table 6.2: Stakeholder feedback results combined

1. The BYOD Management Framework is appropriate in local and district municipality environment regardless of their size.			
Strongly Disagree	Disagree	Agree	Strongly Agree
		30%	70%
2. The different aspects of the BYOD Management Framework are clear and logical.			
Strongly Disagree	Disagree	Agree	Strongly Agree
	4%	46%	50%
3. The BYOD Management Framework is well-organised to be incorporated by the different levels of management (Top management, Middle management, Low-level management) within the organisation.			
Strongly Disagree	Disagree	Agree	Strongly Agree
	4%	42%	54%
4. The BYOD Management Framework is comprehensive in its inclusion of devices, employees, security, awareness and management of BYOD.			
Strongly Disagree	Disagree	Agree	Strongly Agree
	4%	50%	46%
5. The BYOD Management Framework is useful in assisting local and district			

municipality environment in the management of BYOD.			
Strongly Disagree	Disagree	Agree	Strongly Agree
		40%	60%

As mentioned previously, three open-ended questions were also presented to the representatives. These open-ended questions aimed to determine whether there was anything lacking from the BYOD Management Framework, whether anything could be improved, and lastly if there was anything which stood out. It is clear from the responses that some of the representatives disagreed on the relevance of the BYOD Management Framework, as they emphasised that there should be legislation incorporated within the implementation process. This is evident in the results of the questionnaire, where 12% of the representatives disagreed with some aspects of the BYOD Management Framework, such as the legislation of the BYOD Management Framework, amongst others. A comment regarding the above discussion is as follows:

“Thorough research needs to be done in terms of legislation and alignment”

Nevertheless, the majority of the feedback from the representatives was positive and the representatives agreed that the BYOD Management Framework would be applicable to their SMME environments. This is evident in the overall feedback of the questionnaire. Some of the positive comments from the representatives include the following:

“The BYOD Management Framework provides ideas on what a municipality can do to monitor and manage the BYOD devices given to employees in order to secure the company’s information”

“It opened our minds in that we are faced with huge challenges in information protection because of cell phones”

From the discussion above, it can be deduced that the 24 representatives agreed that the BYOD Management Framework is appropriate to be used in SMMEs. Furthermore, the BYOD Management Framework adheres to the four principles of scalability, utility, efficacy,

and quality. Thus, it can be concluded that the BYOD Management Framework is an applicable framework for SMMEs in general.

6.5. Conclusion

The final BYOD Management Framework discussed in the previous chapter, was produced by using the four phases from the research approach. The research approach allowed the researcher to use the first three phases (analysis, design, and evaluation) to develop the BYOD Management Framework. After developing the BYOD Management Framework, it was necessary to complete the fourth and final phase. For that reason, Phase 4 was discussed in this chapter, which consists of the validation of the BYOD Management Framework.

The validation was done in order to determine whether the BYOD Management Framework conforms to the four principles set earlier. In order to do so, the validation was implemented through a workshop spanning over a period of two days. During this workshop, 24 representatives from various SMME environments, such as local and district municipalities, were used to assist the researcher in the validation process. Furthermore, the workshop was divided into two sessions. Concerning the first session, a presentation was done which provided an explanation of the background and related problems associated with the implementation of BYOD in SMMEs. The second session followed by discussing how the BYOD Management Framework and the generic BYOD policy could be utilised in the SMME, or in this case the municipality. Upon completion of the workshop sessions, a survey in the form of a questionnaire was conducted amongst the representatives. The questionnaire consisted of various statements which were used to determine whether the BYOD Management Framework adheres to the set principles of; scalability, utility, efficacy and quality.

Based on the results of the questionnaire, it was determined that the BYOD Management Framework fully adheres to the foregoing principles. This was evident in that the majority of the representatives agreed that the BYOD Management Framework was applicable in their environments. Nevertheless, it can be deduced that there is an overwhelmingly positive response from the representatives to the BYOD Management Framework. With this in mind, the validation process concludes the fourth phase of the research approach. Nonetheless, it is

important to reflect on the study as a whole. Therefore, the following chapter will reflect on the findings of this study in a holistic manner.

Chapter 7: Conclusion:

7.1. Introduction

A final BYOD Management Framework for SMMEs was developed, as described in the previous chapter. Chapter 6 validated the ability of the BYOD Management Framework to conform to the four principles of scalability, utility, efficacy and quality that are core to this study. On completion of the validation of the BYOD Management Framework, it was found that the framework conforms to these four principles and it is, therefore, suitable to be used in an SMME environment. However, it is essential to discuss the findings of the complete study.

This chapter will begin with a discussion on the summary of the study as a whole. The research objectives discussed in Chapter 1 will be analysed in order to confirm whether it was met. Furthermore, this chapter will discuss the research contribution, after which various suggestions for future research will conclude this chapter. Nonetheless, it is important to reflect on the findings of this study in a summative manner.

7.2. Summary of Findings

SMMEs process, communicate and store information to conduct most organisational tasks. Furthermore, employees use information in the decision-making process and conducting their daily tasks. For this reason, information is deemed an important asset in organisations and similarly in SMMEs.

It was emphasised in Chapter 2 that the information utilised in SMMEs and organisations alike is processed, communicated and stored using ICT. Furthermore, ICT is susceptible to risks, such as malware, that could expose the sensitive information to unauthorised users. Exposing this sensitive information to unauthorised users could have a devastating effect on the SMME. Nonetheless, organisations depend on their information to conduct most of their organisational tasks. Thus, it is imperative that the sensitive organisational information is constantly protected. However, unlike large organisations, SMMEs face challenges in this regard. This is most likely due to limited resources and finances, which could affect their ability to protect their information assets properly.

With this said, most modern day organisations are dependent on the use of ICT when conducting their various tasks. As a result, Chapter 3 provided an overview of the history of

some of the revolutionary developments in ICT. One distinct development in ICT is that of mobile devices. A mobile device is a hand-held device that allows users to process, communicate, and store information whilst being on the move. Subsequently, the development of mobile devices has brought in the existence the phenomenon called 'BYOD'.

BYOD is a phenomenon that allows employees to utilise their personal mobile devices to conduct their organisational tasks at work and at home. BYOD is being adopted by most organisations and more specifically, SMMEs. As previously mentioned, SMMEs face various challenges most likely due to limited resources and finances. Thus, the adoption of BYOD in SMMEs will assist in the managing of resources as the employees manage and purchase their own BYOD devices. Consequently, Chapter 3 discussed the influence of BYOD in SMMEs, highlighted a real-life problem that is associated with the use of BYOD in SMMEs, and how SMMEs lack in producing the necessary mechanisms to manage BYOD effectively.

To address the real-life problem identified, Chapter 4 elaborated on a research approach that was defined within the paradigm of design-oriented IS research. This research approach aims to produce an artefact in the form of a framework, which in this case is the BYOD Management Framework. The aim of the BYOD Management Framework is to address the problem at hand.

By using this research approach, Chapter 5 discussed the development of the BYOD Management Framework for SMMEs. The BYOD Management Framework consists of various sections that were developed with the assistance from the class of stakeholders, in this case local government. Local government was chosen due to it having similar characteristics as SMMEs, such as limited resources and finances. Upon the completion of the development of the BYOD Management Framework, it was required to validate the conformance of the BYOD Management Framework to the four previously defined principles of; scalability, utility, efficacy and quality.

Chapter 6 discussed the validation process of the BYOD Management Framework, which was in the form of a two-day workshop. During this workshop, a survey in the form of a questionnaire was distributed amongst 24 representatives from various Local and District Municipalities in the Eastern Cape region of South Africa. After conducting the questionnaire, data from the various responses was gathered and analysed. The results suggested that the

BYOD Management Framework fully conforms to the four stated principles of; scalability, utility, efficacy and quality. As a result, the BYOD Management Framework provides the necessary guidance for the management of BYOD in SMMEs.

7.3. Meeting the Objectives

This study aimed to address a real-life problem identified in SMMEs. Consequently, in Chapter 1, the primary objective aims, *“To formulate a framework towards governing information related risks associated with the rollout of BYOD in an SMME environment”*.

To achieve the primary objective, Chapter 1 identified various secondary objectives that collectively address the real-life problem associated with BYOD in SMMEs. These secondary objectives include the following:

1. To study the information related risks associated with BYOD in a typical SMME environment
2. To identify governance related sources currently in place for BYOD that could be utilised in an SMME environment
3. To formulate a governance-orientated solution towards mitigating information related risks of BYOD in an SMME environment

To *“Study the information related risks associated with BYOD in a typical SMME environment”*, Chapter 3 emphasised that most modern organisations, including SMMEs, permit employees to use their personal mobile devices in order to gain access to personal and organisational information (the phenomenon of BYOD) ‘anywhere’ or ‘anytime’. Furthermore, Chapter 3 added that the use of BYOD devices to gain access information ‘anywhere’ and “anytime” exposes the information to various risks such as malware. Consequently, it is imperative that organisations protect the BYOD devices from the risks associated with BYOD. This addressed the secondary objective set.

After addressing the first secondary objective, it was necessary to, *‘Identify governance related sources currently in place for BYOD that could be utilised in a SMME environment’*. In order to do so, Chapter 5 identified four existing BYOD frameworks (refer to section 5.3.1) that have the intention of managing BYOD in various organisations. Furthermore, the four existing BYOD frameworks were evaluated (subsection 5.3.2) to determine whether it was

relevant to use when developing the contribution framework for SMMEs. Having done this successfully, it can be claimed that the secondary objective has been met.

This led to the third secondary objective, which is to, “*Formulate a governance-orientated solution towards mitigating information related risks of BYOD in an SMME environment*”. In order to do so, Chapter 5 discussed the development of the BYOD Management Framework thereby addressing the third secondary objective.

The secondary objectives highlighted above, collectively address the primary objective of this study which aims to develop the BYOD Management Framework for managing BYOD in SMMEs. Thus, it can be deduced that the objectives of this study were satisfactorily met.

7.4. Summary of Contributions

This study developed three research contributions that collectively represent the entire contribution. The three research contributions consist of; the BYOD Management Framework (artefact), the contextualised research process and academic publications. Each of the three contributions will now be discussed individually.

7.4.1. Research Contribution: The artefact

The first contribution to be discussed is the artefact in the form of a framework (BYOD Management Framework), which was produced in this study. The BYOD Management Framework was developed to address the real-life problem of the information-related risks associated with BYOD in SMMEs (refer to Chapter 1). With the problem identified, the artefact (BYOD Management Framework) was developed as discussed extensively in Chapter 5. Furthermore, it was also highlighted in Chapter 5 that the BYOD Management Framework went through a process of refinement until it was finalised. The finalised BYOD Management Framework consists of six interrelated sections. These six interrelated sections are: BYOD Security Requirements, BYOD Role Players, BYOD Strategy, BYOD Policy Plan, BYOD Policy Implementation, and BYOD Compliance. Figure 7.1 represents the BYOD Management Framework with its six interrelated sections.

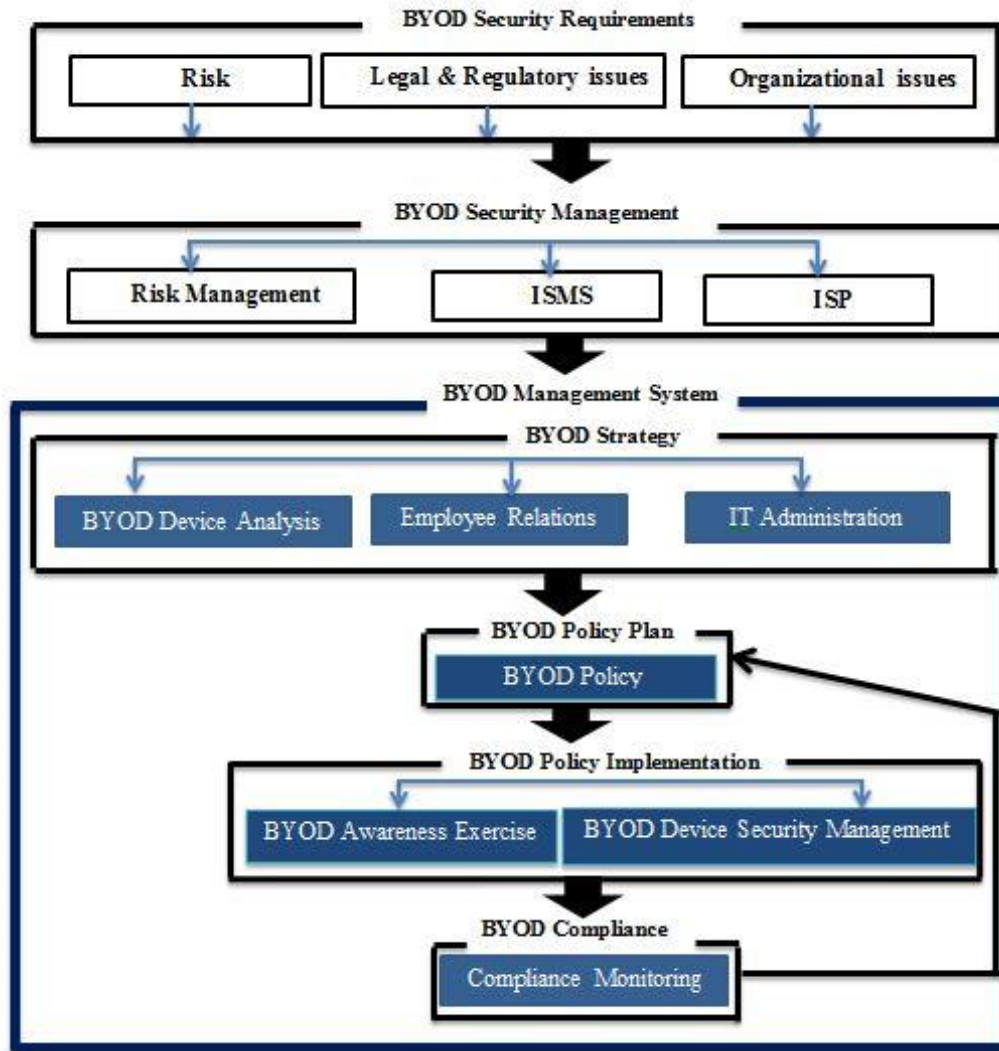


Figure 7.1: Final BYOD Management Framework

The first section at the top of the BYOD Management Framework is the BYOD Security Requirements. The BYOD Security Requirements are where the SMMEs identify any risks to the organisational information when initially implementing BYOD. Furthermore, the SMMEs also consider any legal and regulatory issues and any other security requirements with the initial implementation of BYOD.

The second section, the BYOD Security Management, is dedicated to identifying the risks of BYOD. In order to do so, SMMEs are referred to supporting documentation, such as the ISMS, when making decisions on how the SMME will manage the risks related to BYOD.

The third, fourth, fifth and sixth sections are integrated into the BYOD Management System. This is where the decision-making process takes place and SMMEs decide how they want to

manage BYOD. The aspects in the BYOD Management System recommend that SMMEs should manage BYOD by formulating a strategy. This strategy should take into account the BYOD Devices, Employee Relations and the IT Administration. Upon the completion of the strategy, a BYOD policy is developed and implemented. Following the implementation of the BYOD policy, the SMME can monitor the BYOD users' compliance with the policy.

The complete BYOD Management Framework collectively addressed the primary objective of this study. Furthermore, it is important to note that the development of the BYOD Management Framework was highly dependent on design-oriented IS research. However, the artefact (BYOD Management Framework), has to adhere to four principles to be regarded as design-oriented IS research, as discussed in Chapter 4.

7.4.2. Adherence to Research Paradigm Principles

As discussed in Chapter 4, Österle et al. (2011) proposes four principles for the development of the artefact in design-oriented IS research. The artefact (BYOD Management Framework) has to adhere to the following four principles to be regarded as design-oriented IS research:

- **Abstraction:** The BYOD Management Framework must be applicable to a class of problems.
- **Originality:** The BYOD Management Framework must substantially contribute to the advancement of the body of knowledge.
- **Justification:** The BYOD Management Framework must be justified in a comprehensive manner and validated.
- **Benefit:** The BYOD Management Framework must yield benefit – either immediately or in the future – for the respective stakeholder groups.

Principle of Abstraction

The first principle, which is the principle of Abstraction, states that, “*The BYOD Management Framework must be applicable to a class of problems*”. In other words, the BYOD Management Framework must be applicable to SMMEs in general and not focused on addressing a single SMME. For example, this study validated the BYOD Management Framework through a workshop. During the workshop, 24 representatives from various

SMMEs attended, and not only one SMME representative indicated that the BYOD Management Framework is applicable to a ‘class of problems’. Moreover, it can be argued that the BYOD Management Framework is applicable to South Africa, but it can be extrapolated to similar instances in the rest of the world. This is due to the South African SMME contexts (as discussed in Chapter 3) having similar characteristics as international SMMEs. Therefore, it can be espoused that the BYOD Management Framework has adhered to the principle of Abstraction.

Principle of Originality

The second principle in design-oriented IS research is Originality, which requires that “*The BYOD Management Framework must substantially contribute to the advancement of the body of knowledge*”. Consequently, the BYOD Management Framework is a tailor-made contribution providing SMMEs with guidance on how to manage BYOD effectively. Furthermore, the attendees to the workshop supported this view. This was argued in Chapter 6. Thus, it can be deduced that the BYOD Management Framework effectively conforms to the principle of Originality.

Principle of Justification

The principle of Justification requires that, “*The BYOD Management Framework must be justified in a comprehensive manner and validated*”. Accordingly, the justification for the BYOD Management Framework is provided in Chapter 2 and Chapter 3 where the information-related risks associated with the adoption of BYOD in SMMEs were identified as highlighted. Furthermore, the principle of Justification requires that the BYOD Management Framework be validated. As discussed in Chapter 6, the BYOD Management Framework has been validated indeed. Consequently, due to the aforementioned, the BYOD Management Framework conforms to the principle of Justification.

Principle of Benefit

Considering the last principle, the principle of Benefit, it is required that, “*The BYOD Management Framework must yield benefit – either immediately or in the future – for the respective stakeholder groups*”. Accordingly, the BYOD Management Framework has been deemed beneficial to the stakeholders. This is evident from Chapter 6 where it was

emphasised that the representatives of the workshop concurred that the BYOD Management Framework will provide great benefit to the SMME landscape. One of the representatives from the workshop further supports this by stating:

“The BYOD Management Framework is useful in addressing the risks associated with BYOD because it is clear and understandable, which means that it can be easily applied in the municipal environment”

Taking the aforementioned statement into consideration, it can be contended that the BYOD Management Framework adheres to the principal of Benefit.

With this in mind, it is clear that this study can indeed be classified as design-oriented IS research. This is due to the fact that the artefact (the BYOD Management Framework) fully adheres to the four principles of design-oriented IS research.

7.4.3. Methodological Contribution

The second research contribution is in the form of a methodological contribution. Chapter 4 discussed that the initial research paradigm was design-oriented IS research. Unfortunately, design-oriented IS research does not provide detailed guidance on how to conduct the intended research. However, design-oriented IS research does provide the researcher with some form of academic freedom. For this reason, it became clear that another paradigm should be consulted, which is the paradigm of design-based research. The objective of the design-based research is very similar to that of design-oriented IS research, that of producing an artefact.

Although design-based research and design-oriented IS research are very similar, design-based research provides comprehensive guidance on the steps to conduct the associated research process. Consequently, design-oriented IS research and design-based research were utilised to support each other. In doing so, design-based research and design-oriented IS research was contextualised to formulate a contextualised research process that was used in this study (as discussed extensively in Chapter 4). Notwithstanding the above discussion, other researchers with similar research studies to this study can possibly use the methodological contribution.

7.4.4. Academic Publications

Concerning the first published paper, an international conference paper was published in the proceedings of the 2016 IST-Africa Conference, held in Durban, South Africa. The first paper drew from literature to highlight the preliminary results of the risks associated with the adoption of BYOD in SMMEs. This paper was written during the initial phase of this study (Phase 1).

The second paper was published by a local conference in the proceedings of the 2016 Information Security South Africa (ISSA) Conference, held in Johannesburg, South Africa. The published proceedings took place in Johannesburg, South Africa. The paper provided details on the process of the development of the BYOD Management Framework. In view of the above, the conference papers are referenced below.

- Fani, N., Von Solms, R., & Gerber, M. (2016). Governing Information Security Within the Context of “ Bring Your Own Device in SMMEs .” In *IST-Africa* (pp. 1–11). Retrieved from <http://ieeexplore.ieee.org/abstract/document/7530586/?reload=true>
- Fani, N., Von Solms, R., & Gerber, M. (2016). A framework towards governing “Bring Your Own Device in SMMEs.” In *ISSA Conference*.

Taking the above into consideration, the three contributions of the BYOD Management Framework (artefact contribution, the contextualised research process and academic publications), collectively served as the research contribution of this study. Nevertheless, it is important to consider any future research.

7.5 Future research

The BYOD Management Framework took into account the aspect of legal and regulatory issues. However, it was highlighted in Chapter 6 that some of the workshop representatives challenged the aspect of legal and regulatory issues. In turn, the representatives recommended that in-depth research is required on how to address the legislation issues in SMMEs. Therefore, future research is required that mainly focus on handling the legislation issues associated with BYOD in SMMEs. This is supported by the following statement provided by the representatives, as highlighted in Chapter 6:

“Thorough research needs to be done in terms of legislation and alignment of legislation to BYOD”

Taking into account the aforementioned, any future research will be beneficial in this regard.

7.6. Epilogue

This study investigated the context of BYOD in SMMEs. Most SMMEs are adopting BYOD, however, these SMMEs are not effectively managing the risks associated with BYOD. With this in mind, this study identified the existence of contributions towards the management of BYOD. Unfortunately, these contributions did not take into consideration the SMME environments. Consequently, SMMEs faced various challenges with regards to effectively managing BYOD.

With this in mind, this study developed an artefact in the form of a framework (BYOD Management Framework). In producing the BYOD Management Framework, this study aimed at addressing the lack of adequate management of BYOD in SMMEs. In doing so, this study contributed to the management of BYOD in SMMEs. As a result, this study achieved its aim of producing an artefact in the form of a framework (BYOD Management Framework) that was relevant to the SMMEs in general. Furthermore, this study achieved its aim of producing the BYOD Management Framework that conformed to the four principles of; scalability, utility, efficacy and quality.

As a result, it can be claimed that the BYOD Management Framework is scalable and usable in the various SMMEs, regardless of their size. Furthermore, the BYOD Management Framework provides value to the SMMEs, as it was tailor-made to suit the specific needs of their environments.

References

- 2013 Norton Report. (2013). <http://doi.org/07/04/2015>
- Aakanksha, B. B. G., Ankit, T., Jain, K., & Agrawal, D. P. (2016). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*. <http://doi.org/10.1007/s00521-016-2275-y>
- Abor, J., & Quartey, P. (2010). Issues in SME Development in Ghana and South Africa. *International Research Journal of Finance and Economics*, 39(39), 218–228. <http://doi.org/ISSN 1450-2887>
- Agar, J. (2013). *Constant Touch: A Global History of the Mobile Phone*.
- Allam, S., & Flowerday, S. (2011). An adaptation of the awareness boundary model towards smartphone security. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. <http://doi.org/10.1109/ISSA.2011.6027527>
- Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, 42, 55–65. <http://doi.org/10.1016/j.cose.2014.01.005>
- Ambika, D., & Radha, V. (2012). Secure Speech Communication – A Review. *International Journal of Engineering Research and Applications*, 2(5), 1044–1049.
- Andrew, B. (2012). *TCO & Security of Enterprise Grade Mobility*.
- Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, 14(2), 346–352.
- Attaran, M. (2004). Exploring the relationship between information technology and business process reengineering. *Information and Management*, 41(5), 585–596. [http://doi.org/10.1016/S0378-7206\(03\)00098-3](http://doi.org/10.1016/S0378-7206(03)00098-3)
- AV-TEST Malware Statistics. (2016). Retrieved from <https://www.av-test.org/en/statistics/malware/>
- Baecker, R. M., & Kaufmann, M. (2014). *Readings in Human-Computer Interaction: Toward the Year 2000*.
- Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C., & Horst, G. (2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices, (March 2010). <http://doi.org/10.1109/SP.2011.29>

- Bhat, C. R., Dalal, P., Deutsch, K., Goulias, K. G., Hu, H.-H., Lei, T., ... Yoon, S. Y. (2010). DEVELOPMENT OF OPPORTUNITY-BASED ACCESSIBILITY INDICATORS. *Transportation Research Record*, (702), 1–19.
- Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. *IEEE Communications Magazine*, 39(12), 86–94. <http://doi.org/10.1109/35.968817>
- Boote, D. N., & Beile, P. (2005). Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation, 34(6), 3–15.
- Borek, A., Kumar Parlikad, A., Webb, J., & Woodall, P. (2013). *Total Information Risk Management: Maximizing the Value of Data and Information Assets*. Newnes.
- Botha, A., Makitla, I., Ford, M., Fogwill, T., Seetharam, D., Abouchabki, C., ... Oguneye, O. (2009). The mobile phone in Africa : Providing services to the masses.
- Broadbent, M. (1998). The phenomenon of knowledge management : What does it mean to the information profession ? *Information Outlook*, 2(5), 23–26,28–30,32, 34–36.
- Brodin, M. (2015a). Combining ISMS with strategic management: the case of BYOD
COMBINING ISMS WITH STRATEGIC MANAGEMENT: THE CASE OF BYOD, (August).
- Brodin, M. (2015b). Management issues for Bring Your Own Device.
- Brody, R. G., Mulig, E., Florida, S., Petersburg, S., Kimball, V., Florida, S., & Petersburg, S. (2007). PHISHING , PHARMING AND IDENTITY THEFT, 11(3), 43–56.
- Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, 11(3), 43–56.
- Caldwell, T. (2011). Data loss prevention - Not yet a cure. *Computer Fraud and Security*, 2011(9), 5–9. [http://doi.org/10.1016/S1361-3723\(11\)70089-6](http://doi.org/10.1016/S1361-3723(11)70089-6)
- Charbonneau, S. (2011). The role of user-driven security in data loss prevention. *Computer Fraud and Security*, 2011(11), 5–8. [http://doi.org/10.1016/S1361-3723\(11\)70112-9](http://doi.org/10.1016/S1361-3723(11)70112-9)
- Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses, 1(1), 247–256.
- Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing, (973), 647–651. <http://doi.org/10.1109/ICCSEE.2012.193>
- Companies Act (2009). Retrieved from <https://www.google.co.za/url?sa=t&source=web&rct=j&url=http://www.cipc.co.za/index.p>

hp/download_file/view/257/152/&ved=0ahUKEwjCrKTQuOTSAhVklMAKHRcmDalQFggqMAI&usg=AFQjCNGw86PIx1Xfi-pX8k2idNOzEyGKrA

- Coulson, T., & Zhu, J. (2005). The Price of Security : The Challenge of Measuring Business Value Investments in Securing Information Systems Investments in Securing Information Systems, 5(4).
- Crees, J., & Self, R. (2013). IS Practices for SME Success Series The Role of Enterprise Systems, 82. <http://doi.org/10.1093/itnow/bws010>
- Crowley, D., & Heyer, P. (2015). *Communication in History: Technology, Culture, Society*.
- Dang-pham, D., & Pittayachawan, S. (2014). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university : A Protection Motivation Theory approach. *Computers & Security*, 48, 281–297. <http://doi.org/10.1016/j.cose.2014.11.002>
- Davies, M. (2011). Concept mapping, mind mapping and argument mapping: What are the differences and do they matter? *Higher Education*, 62, 279–301. <http://doi.org/10.1007/s10734-010-9387-6>
- Dedeche, A. A., Liu, F., Le, M., & Lajami, S. (2013). Emergent BYOD Security Challenges and Mitigation Strategy Research Methodology, 1–17.
- Devos, J., Landeghem, H. Van, Deschoolmeester, D., & Devos, J. (2012). Rethinking IT governance for SMEs. *Emerald*. <http://doi.org/10.1108/02635571211204263>
- Dulaney, K., & Debeasi, P. (2011). Thou Shalt Allow BYOD. Retrieved from https://www.google.co.za/url?sa=t&source=web&rct=j&url=http://www.informationweek.com/pdf_whitepapers/approved/1338556417_eb_MaaS360_10CommandmentsFINAL.pdf&ved=0aHUKewiFh6Wku-TSAhXsK8AKHafvA0oQFggqMAA&usg=AFQjCNFoyD73PZ7-aWTZHMaz9WNtZgFMsgq
- El-Tawy, N., & Abdel-Kader, M. (2012). Accounting recognition of information as an asset. *Journal of Information Science*, 39(3), 333–345. <http://doi.org/10.1177/0165551512463648>
- Eslahi Meisam, & Var Naseri Maryam. (2014). BYOD: The Current State and Security Challenges. *IEEE Symposium on Computer Applications & Industrial Electronics*, 189–192.
- Fakhrutdinova, E., Kolesnikova, J., Yurieva, O., & Kamasheva, A. (2013). The Commercialization of Intangible Assets in the Information Society. *World Applied Sciences Journal*, 27, 82–86. <http://doi.org/10.5829/idosi.wasj.2013.27.emf.17>
- Forrester. (2012). Key Strategies To Capture And Measure The Value Of Consumerization Of IT, (May).

- French, A. M., Guo, C., & Shim, J. P. (2014). Current Status , Issues , and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems*, 35.
- Gandotra, P., & Kumar, R. (2016). Device-to-Device Communication in Cellular Networks : A Survey. *Journal of Network and Computer Applications*, 71, 99–117. <http://doi.org/10.1016/j.jnca.2016.06.004>
- Garba, A. B., Armarego, J., & Murray, D. (2015). BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY, 10(3), 1279–1287.
- Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal of Information Privacy and Security*, 11(1), 38–54. <http://doi.org/10.1080/15536548.2015.1010985>
- Gessner, D., Girao, J., Karame, G., & Li, W. (2013). Towards a user-friendly security-enhancing BYOD solution. *NEC Technical Journal*, 7(3), 113–116.
- Ghosh, A., & Rai, P. K. G. S. (2013). Bring Your Own Device (Byod): Security Risks and Mitigating Strategies. *Journal of Global Research in Computer Science*, 4(4), 62–70.
- Goggin, G. (2012). *Cell Phone Culture: Mobile Technology in Everyday Life*.
- Goldstuck Arthur. (2012). *Internet Matters*.
- Grillmayer, L., Dipl, S., & Wachs, M. (2013). Radio-Frequency Identification - Overview, (February), 25–33. <http://doi.org/10.2312/NET-2013-02-1>
- Harris, M., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22, 97–114. <http://doi.org/10.1108/IMCS-03-2013-0019>
- Harris, M., Patten, K., & Regan, E. (2013). The Need for BYOD Mobile Device Security Awareness and Training. In *Proceedings of the Nineteenth Americas Conference on Information Systems*.
- Hensema, M. (2013). Acceptance of BYOD among Employees at Small to Medium-sized Organizations. *19th Twente Student Conference on IT*, 1 – 8.
- Herrington, J., Mckenney, S., Reeves, C. T., & Oliver, R. (2005). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal.
- HPE Security Research Cyber Risk Report. (2016), 1–96.

- ISACA. (2010). Data Leak Prevention, (September), 1–14. Retrieved from <http://www.isaca.org/Knowledge-Center/Research/Documents/DLP-WP-14Sept2010-Research.pdf>
- ISO 27002. (2013). Retrieved from https://www.google.co.za/url?sa=t&source=web&rct=j&url=http://www.iso27001security.com/html/27002.html&ved=0ahUKEwjW_d71weTSAhVrl8AKHXAdDC8QFggYMAA&usg=AFQjCNG8ml6j7WtffDI2R8FpE5Ei_6BNqw
- Johnson, S., Twilley, N., Zhang, T., Zhou, Z., & Wu, S. (n.d.). A look at concepts , problems , and solutions.
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leverage threats to the human asset through sanctioning rhetoric, 39(1), 113–134.
- Kamboj, V., & Gupta, H. (2012). Mobile Operating Systems, 1(2), 169–174.
- Kew, J., Herrington, M., & Hooper, V. (2010). The use of Mobile Phones by SMMEs in a Developing Economy : The Case in South Africa.
- Kew, P., & Herrington, M. (2015). *Global Entrepreneurship Monitor (GEM): South African Report*.
- Keyes, J. (2013). Bring Your Own Devices (BYOD) Survival Guide, 6(13), 451. <http://doi.org/10.1201/b14050>
- Khan, A. (2014). Government Funds Available to SMEs in South Africa. *The Journal of the Global Accounting Alliance*.
- Khan, Q., Butt, M. A., Zaman, M., & Asger, M. (2013). A Novel Approach Based Information Integrity Modeling, 2(1), 210–215.
- Koltay, T. (2011). The media and the literacies: media literacy, information literacy, digital literacy. *Media, Culture & Society*, 33(2), 211–221. <http://doi.org/10.1177/0163443710393382>
- Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices. *Amcis*, (2008), 1–8. Retrieved from <http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/>
- Leonardi, P. M., Huysman, M., & Steinfield, C. (2013). Enterprise Social Media : Definition , History , and Prospects for the Study of Social Technologies in Organizations, 19, 1–19. <http://doi.org/10.1111/jcc4.12029>

- Lewis, V. L., & Churchill, N. C. (1983). *The Five Stages of Small Business Growth*.
- Lindsay, A., Downs, D., & Lunn, K. (2003). Business processes — attempts to find a definition, 45, 1015–1019. [http://doi.org/10.1016/S0950-5849\(03\)00129-0](http://doi.org/10.1016/S0950-5849(03)00129-0)
- Littlejohn, S. W., & Foss, K. A. (2010). *Theories of Human Communication* (tenth).
- Loose, M., Weeger, A., & Gewald, H. (2013). BYOD—The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption Behavior from the Perspective of Future Employees. *Amcis*, 1–12. Retrieved from <http://aisel.aisnet.org/amcis2013/EndUserIS/GeneralPresentations/12/>
- Macgregor, G., & Macgregor, G. (2006). The nature of information in the twenty-first century. <http://doi.org/10.1108/00242530510574129>
- Madzima, K., Moyo, M., & Abdullah, H. (2014). Is Bring Your Own Device an institutional information security risk for small-scale business organisations ?
- Masadeh, M. a. (2012). Focus Group : Reviews and Practices. *International Journal of Applied Science and Technology*, 2(10), 63–68.
- Merad, M., Dechy, N., Serir, L., Grabisch, M., & Marcel, F. (2013). Using a multi-criteria decision aid methodology to implement sustainable development principles within an organization. *European Journal of Operational Research*, 224(3), 603–613. <http://doi.org/10.1016/j.ejor.2012.08.019>
- Mervyn, K. (2009). King III report.
- Metropolis, N., Howlett, J., & Rota, G.-C. (2014). *History of Computing in the Twentieth Century*.
- Mittleman, D., French, A. M., Welke, R., & Guo, J. C. (2013). Bring Your Own Device (BYOD): Current Status , Issues , and Future Directions.
- Moberly, M. D. (2014). *Safeguarding intangible assets*. Butterworth-Heinemann.
- Monreale, A., Rinzivillo, S., Pratesi, F., Giannotti, F., & Pedreschi, D. (2014). Privacy-by-design in big data analytics and social mining, 1–26.
- Moody, D., & Walsh, P. (1999). Measuring The Value Of Information: An Asset Valuation Approach. *Seventh European Conference on Information Systems (ECIS'99)*, 1–17. <http://doi.org/citeulike:9316228>
- Myers, B. A. (1996). A Brief History of Human Computer Interaction Technology, 28(December).

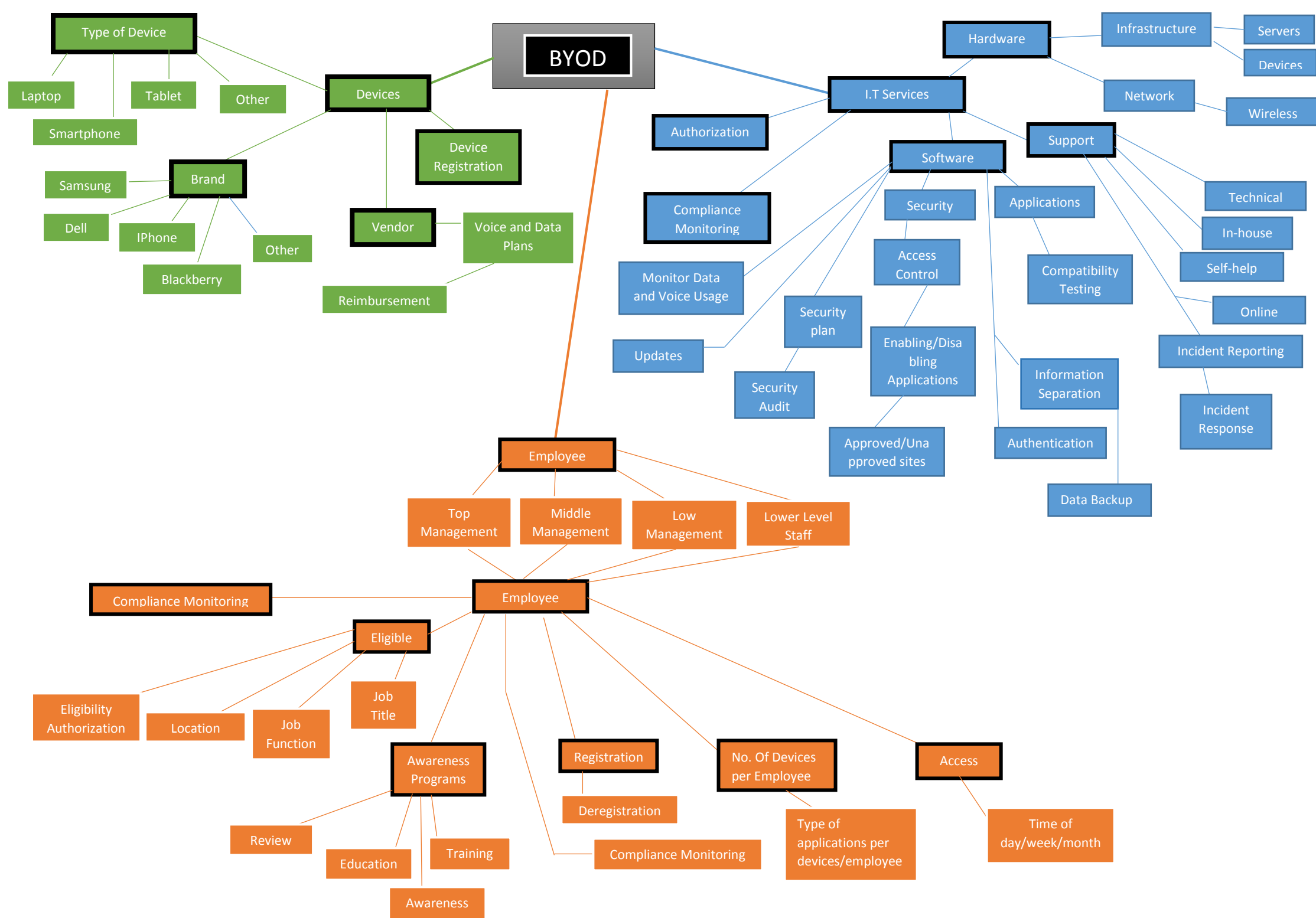
- National Small Business Amendment Act (2004). South Africa. Retrieved from <https://www.google.co.za/url?sa=t&source=web&rct=j&url=http://www.gov.za/documents/national-small-business-amendment-act&ved=0ahUKEwjDzJPkvuTSAhXLDcAKHTCfAVoQFggIMAI&usg=AFQjCNFbCsi-zQdJpkV5ITNMfhW66zmP0w>
- Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization – A Theory and Practice Review. In *Proceedings of the 18th Americas Conference on Information Systems*.
- Okello-Obura, C., & Matovu, J. (2011). SMEs and Business Information Provision Strategies: Analytical Perspective, Dr. *Library Philosophy and Practice*.
- Olalere, M., Abdullah, M. T., Mahmood, R., & Abdullah, a. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 5(2). <http://doi.org/10.1177/2158244015580372>
- Ollmann, G. (2007). *The Phishing Guide: Understanding & Preventing Phishing Attacks*.
- Ommen, B. (2014). IT Security in SMEs: Necessary or Irrelevant? Retrieved from <http://referaat.cs.utwente.nl/conference/21/paper/7442/it-security-in-smes-necessary-or-irrelevant.pdf>
- Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., ... Sinz, E. J. (2011). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, 20(1), 7–10. <http://doi.org/10.1057/ejis.2010.55>
- Owens, L. K. (2002). Introduction To Survey Research Design Why Do a Survey? *SRL Fall 2002 Seminar Series*. Retrieved from <http://www.srl.uic.edu>
- Pachauri, A. K., & Singh, O. (2012). 5G Technology – Redefining wireless Communication in upcoming years, *I(1)*, 12–19.
- Perssonneault, A., & Kraemer, K. L. (2014). Survey Research Methodology in Information Systems Management: An Assessment. *Journal of Management Information Systems*, 10(2), 75–105.
- Pillay, a, Nham, E., Tan, G., & Diaki, H. (2013). *Does BYOD increase risks or drive benefits?* Retrieved from <http://hdl.handle.net/11343/33345>
- Pinzon, S. (2008). Top 10 Threats to SME Data Security (and what to do about them). *October*, 1–3.
- Poyatos, F. (2008). *Textual Translation and Live Translation: The Total Experience of Nonverbal Communication in Literature, Theater and Cinema*.
- PWC. (2016). *PWC Global State of Information Security Survey*.

- Ramu, S. (2012). Mobile Malware Evolution , Detection and Defense, (April), 1–15.
- Rao, U. H., & Nayak, U. (2014). The InfoSec Handbook An Introduction to Information Security. In *Apress*. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4302-6383-8_16/fulltext.html
- Redman, T. C. (2008). *Data Driven: Profiting from Your Most Important Business Asset*. United States of America: Harvard Business Press. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=Y0G6HpIMbVUC&oi=fnd&pg=PR7&dq=Information+as+an+important+business+asset&ots=WsfHx57w9f&sig=1O9WmrEAzOUP_YiGKzmWH1_rmos#v=onepage&q=Information as an important business asset&f=false
- RSA Online Fraud Resource Centre. (2014). Retrieved from <http://southafrica.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm>
- SAICA. (2015). *2015 SME Insights Report*.
- Sapakal, M. R. S., & Kadam, M. S. S. (2013). 5G Mobile Technology, 2(2), 568–571.
- Scarfo, A. (2012). New security perspectives around BYOD. *Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012*, 446–451. <http://doi.org/10.1109/BWCCA.2012.79>
- Self, R., & Kestle, R. (2013). *IS Practices for SME Success Series. IS Practices for SME Success Series* (Vol. 1).
- Selviandro, N., Wisudiawan, G., Puspitasari, S., & Adrian, M. (2015). Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control. In *2015 3rd International Conference on Information and Communication Technology (ICoICT)* (pp. 113–118). <http://doi.org/10.1109/ICoICT.2015.7231407>
- Shahzad, A., Hussain, M., Naeem, M., & Khan, A. (2013). Protecting from Zero-Day Malware Attacks, 17(4), 455–464. <http://doi.org/10.5829/idosi.mejsr.2013.17.04.12159>
- Shaikh, A. a., & Karjaluo, H. (2015). Making the most of information technology & systems usage: A literature review, framework and future research agenda. *Computers in Human Behavior*, 49, 541–566. <http://doi.org/10.1016/j.chb.2015.03.059>
- Sharma, P. (2013). Evolution of Mobile Wireless Communication Networks-1G to 5G as well as Future Prospective of Next Generation Communication Network, 2(August), 47–53.
- Sheridan, J., Ballagas, R., & Rohs, M. (2004). BYOD: bring your own device. *Procedia Technology*, 9, 43–53. <http://doi.org/10.1016/j.protcy.2013.12.005>

- Soni, P., Cowden, R., & Karodia, A. M. (2015). INVESTIGATING THE CHARACTERISTICS AND CHALLENGES OF SMMES IN THE ETHEKWINI METROPOLITAN MUNICIPALITY, 3(10), 15–93.
- Suhail Qadir Mir, Mehraj-ud-din Dar, S M K Quadri, B. M. B. (2011). Information availability: Components, Threats and Protection mechanisms. *Journal of Global Research in Computer Science*, 2(3).
- Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards : A Comparative Study of the Big Five Information Security Management System Standards : A Comparative Study of the Big Five, (January 2016).
- Swanson, M., & Guttman, B. (1996). NIST 800-12, 60. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>
- Tatnall, A. (n.d.). HISTORY OF COMPUTER HARDWARE AND SOFTWARE DEVELOPMENT. In *Encyclopedia of Life Support Systems (EOLSS)*.
- Twinomurinzi, H., & Mawela, T. (2014). Employee perceptions of BYOD in South Africa : Employers are turning a blind eye ?, 126–131.
- Valdez-juárez, L. E., Lema, D. G. De, & Maldonado-guzmán, G. (2016). Management of Knowledge , Innovation and Performance in SMEs, 11, 141–176.
- Vaus, D. de. (2002). *Surveys in Social Research* (5th ed.). Australia: Allen & Unwin. Retrieved from http://books.google.co.za/books?id=x6Vp5NO93CAC&printsec=frontcover&source=gbg_summary_r&cad=0#v=onepage&q&f=false
- Vishwanath, A. (2016). Computers in Human Behavior Mobile device affordance : Explicating how smartphones in fl uence the outcome of phishing attacks, 63, 198–207. <http://doi.org/10.1016/j.chb.2016.05.035>
- Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), 80–85. <http://doi.org/10.1109/CCNC.2014.6866552>
- Weeger, A., & Gewald, H. (2014). Factors Influencing Future Employees Decision-Making to Participate in a BYOD Program: Does Risk Matter? *Proceedings of the European Conference on Information Systems (ECIS)*, 0–14.
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (fourth).
- Widen-Wulff, G. (2004). Explaining knowledge sharing in organizations through the dimensions of social capital. *Journal of Information Science*, 30(5), 448–458. <http://doi.org/10.1177/0165551504046997>

- Wilbanks, W. G. (1996). 50 years of progress in measuring and controlling industrial processes. *IEEE Control Systems*.
- Winston, B. (1998). *Media Technology and Society: A History: from the Telegraph to the internet*.
- World Economic Forum. (2012). *Global risks 2012. Insight report*. Retrieved from <http://www.weforum.org/reports/global-risks-2012-seventh-edition>
- Xesha, D., Iwu, C. G., & Slabbert, A. (2014). Business Relationships as a Driver of Success for Small , Medium , and Micro Enterprises (SMMEs) in South Africa, 5(1), 37–43.
- Xu, J. H. (2016). Media Discourse on Cell Phone Technology and “ Left-Behind Children ” in China, 9(1), 87–102.
- Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013). Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior. *Proceedings - SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013*, 411–416. <http://doi.org/10.1109/SocialCom.2013.64>
- Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., & Groß, T. (2014). Consumerisation of IT : Mitigating risky user actions and improving productivity with nudging. *Procedia Technology*, 16, 508–517. <http://doi.org/10.1016/j.protcy.2014.10.118>
- Zafar, H. (2013). Human Resource Management Review Human resource information systems : Information security concerns for organizations. *Human Resource Management Review*, 23(1), 105–113. <http://doi.org/10.1016/j.hrmr.2012.06.010>
- Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework & its analysis. *Computers & Security*, 55, 81–99. <http://doi.org/10.1016/j.cose.2015.06.011>

Appendix A: Mind Map



Appendix B: Questionnaire

Bring Your Own Device (BYOD) / Bring Your Own Municipal Device (BYOMD)

The purpose of this questionnaire is to determine the municipal requirements for BYOD.

Please

answer the questionnaire by choosing from the dropdown list in the **Answer** column or by providing an details in the **Comment** column.

Question	Answer	Justification
1. Devices		
1.1.) Type of Devices:		
1.1.1.) Which type of mobile devices are currently used within the municipality?		
1.2. Device Registration:		
1.2.1.) Which type of brands are currently used for mobile devices?		
1.2.2.) Who is currently responsible for authorizing users who receive the mobile device?		
1.2.3.) Who is responsible for registering the mobile devices?		
1.3.) Vendor:		
1.3.1.) Who is the current vendor for data and voice services?		
1.3.2.) Does the municipality allow employees to make use of their own personal mobile devices to complete business tasks?		
1.3.3.) If Yes , are the employees reimbursed for voice and data costs?		
2. Employee		
2.1.) Eligible:		
2.1.1.) What makes an employee eligible to receive a mobile device from the municipality?		
2.1.2.) What makes an employee not eligible to receive a mobile device from the municipality?		
2.1.3.) Who is responsible for approving the eligible users?		
2.2) No.Of Devices per Employee:		
2.2.1) How many devices can an employee receive?		
2.2.2.) If the answer to the above question is more than one OR two , what makes an employee eligible to receive more than one mobile device? Please provide details in the justification column		
2.3.) Registration:		
2.3.1.) Who is responsible for registering the eligible users?		
2.3.2.) Are employees able to self enrol themselves?		
2.3.3.) If Yes , who is responsible ensuring that self-enrolled employees are enrolled?		
2.3.4) Are there other options for registration provided?		
2.3.5.) If Yes , please provide the options in the justification column		
2.3.6) How are employees deregistered? Please provide options in the justification column		
2.3.7.) What happens to the organizational information when the employee resigns/contract terminated? Please provide details in the justification column		
2.4.) Access:		
2.4.1.) Are there specific hours a municipal employee can access information outside office hours?		
2.4.2) If Yes , please provide the access times in the justified column?		
2.4.2.) Which information can an employee currently access?		





















2.4.3.) Are employees allowed to access their personal applications?		
2.4.4.) If Yes , please provide the access times in the justified column?		
2.4.5.) Will the employee be able to use their BYOD device when travelling?		
2.4.6.) If No , will the organization reimburse the employee?		
2.4.7) What are the terms currently for reimbursing an employee? Please provide details in the justification column		
2.5.) Compliance Monitoring:		
2.5.1.) Is there a document currently which states acceptable use of devices for employees?		
2.5.2.) Are employees aware of this acceptable use document?		
2.5.3.) Does and employee have to sign the acceptable use document?		
2.5.4.) Who is responsible for compliance monitoring?		
2.6.) Awareness Programs:		
2.6.1.) Have the employees been educated on how to secure the organizations information?		
2.6.2.) Which eductaion/awareness programs are currently in place?		
2.6.3.) Have the eductaion/awareness programs assisted in making the employees more secure?		
3.) I.T. Services:		
3.1.) Security:		
3.1.1.) Who is responsible for securing the mobile devices?		
3.1.2.) If the employee is responsible for security, how is the organizational information protected? Please provide details in the justification column		
3.2.) Support:		
3.2.1.) Are there different services provided for support?		
3.2.2.) If Yes, please provide the services in the justification column		
3.2.3.) To whom do employees report incidents like hacking, lost devices etc. ?		
3.3.) Information seperation:		
3.3.1.) Is the personal and organizational information seperated?		
3.3.2.) If Yes , what are the tools in place used to separate the information? Please provide details in the justification column		
3.4.) Updates:		
3.4.1.) How often are mobile devices updated?		
3.4.2.) Who will be responsible for the updates?		
3.4.3.) Are updates manual or automatic?		
3.4.5.) Is there an antivirus installed in smartphones and tablets?		
3.5) Authentication:		
3.5.1) Who is responsible for authenticating users who have access to the organizational information?		
3.5.2) How are users currently authenticated on their mobile devices?		
3.6) Access control:		
3.6.1) Who is currently responsible for managing access?		
3.6.2) What are some of the restrictions in place for access? Please provide details in the justification column		

3.6.3) What happens when there is unauthorized access? Please provide details in the justification column		
3.7) Authorization:		
Who is responsible for authorizing access to municipal information?		
3.8.) Monitor:		
What are some of the activities on mobile devices currently monitored? Please provide details in the justification column		
How are the activities monitored? Please provide details in the justification column		
3.9) Reporting:		
What is the process of reporting for handling stolen or lost devices? Please provide details in the justification column		
What is the process of decommissioning of a device? (e.g. a new device, employee resigns etc.) Please provide details in the justification column		
Will all the data in the device be wiped?		
3.10) Compliance:		
How is employee compliance currently monitored?		
Who will be responsible for monitoring compliance?		
Are IT system tools used to check compliance?		

Appendix C: Questionnaire (Validation of the artefact)

Thank you for participating in the workshop session for: Governing information security within the context of “Bring Your Own Device” in Local Government. Please be so kind as to complete the following questions, so we can further improve on the exercises you have completed today.

Mark with - X

1. The BYOD Management Framework is appropriate in local and district municipality environment regardless of their size.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
2. The different components of the BYOD Management Framework are clear and logical.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
3. The BYOD Management Framework is well-organized to be incorporated by the different levels of management (Top management, Middle management, Low level management) within the organization.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
4. The BYOD Management Framework is comprehensive in its inclusion of devices, employees, security, awareness and management of BYOD.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 
5. The BYOD Management Framework is useful in assisting local and district municipality environment in the management of BYOD.			
Strongly Disagree 	Disagree 	Agree 	Strongly Agree 

6. What have you found to be particularly good and/or useful about the BYOD Management Framework?

7. In what aspects, in your opinion, is the BYOD Management Framework lacking?

8. In your opinion, what aspects about the BYOD Management Framework can be improved?

Appendix D: BYOD Policy



BYOD Policy

Draft policy

Table of Contents

Definition:	3
Scope:	3
1. BYOD Device Analysis:	3
1.1 Authorization:	3
1.2 Type of Device:	3
1.3 Device Registration:	3
1.4 Vendor:	3
2. Employee Relations:	4
2.1 Eligibility:	4
2.2 Registration:	4
2.3 Deregistration:	4
2.4 Number of devices per employee:	4
2.5 Access:	4
2.6 Awareness Programs:	5
2.7 Compliance Monitoring:	5
3. IT Administration:	5
3.1 Authorization:	5
3.2 Authentication:	5
3.3 Communication:	5
3.4 Security:	5
3.4.1 Access control:	5
3.4.2 Information separation:	5
3.4.3 Support:	6
3.4.4 Reporting:	6
3.4.5 Updates:	6
3.4.6 Monitoring:	6
3.4.7 Device and Application Management/Security:	6
3.4.8 Compatibility Testing:	6

Definition:

BYOD: Acronym for **B**ring **Y**our **O**wn **D**evice.

When an employee brings their own personal devices to be made available and used by the municipality.

Scope:

The policy will be applicable to all employees and authorized users who own a mobile device or are in possession of a municipal mobile device. It also covers all mobile devices.

The policy will cover:

- BYOD Device Analysis
- Employee Relations
- IT Administration

1. BYOD Device Analysis:

1.1 Authorization:

1.1.1. Only users who are deemed eligible should go through the necessary route to acquire authorization from the administrator of BYOD.

1.2 Type of Device:

1.2.1. The type of devices to be used by the municipality will be specific to each municipality. The

type of devices can include but is not limited to the following:

- Laptop
- Smartphone
- Tablet

1.3 Device Registration:

1.3.1. Authorized mobile devices to be used for BYOD must be registered.

1.4 Vendor:

1.4.1. The municipality will be responsible for acquiring mobile devices that are not personally

owned by BYOD users.

1.4.2. Users with personally owned devices will be responsible for purchasing their mobile device.

1.4.3. Voice and data plans and costs will be acquired for users who meet the following requirements:

- Use your mobile device mostly outside the municipal offices.
- Users frequently travelling within the country, or overseas.
- Users who need frequently require access to the municipal information anywhere, anytime.

2. Employee Relations:

2.1 Eligibility:

2.1.1. Employees are divided into three different levels; Strategic level, Tactical level and Operational level. Therefore, eligible users for BYOD will be categorized by these levels. Criteria that determine who is eligible to make use of BYOD is:

- Job title
- Job function
- Location

2.2 Registration:

2.2.1. When a user is eligible, they will go through the process of registration. Users will need to communicate with their respective manager or supervisor.

2.3 Deregistration:

2.3.1. When a user is retires, is suspended or resigns from the municipality, they will go through the process of deregistration. When a user is deregistered, the following will occur:

- User rights will be revoked
- If the mobile device is a municipal device, it will be revoked
- All municipal data will wiped from the mobile device

2.4 Number of devices per employee:

The number of devices to be used per employee will be determined by: job title or job function

2.5 Access:

2.5.1. Accessibility is only permitted to registered BYOD users. BYOD users can access the municipal network anytime during the municipal hours. For after working

hour's accessibility, communicate with the BYOD administrator.

2.6 Awareness Programs:

2.6.1. The municipality is dedicated to awareness programs for BYOD. The aim of the awareness programs is to form a culture which makes users aware of how to protect the municipal network and information at all times.

2.7 Compliance Monitoring:

2.7.1. Users are encouraged to comply with the policy at all times. Action will be taken on any users who don't comply with the policy. Action will range from suspension or deregistration of users.

3. IT Administration:

3.1 Authorization:

3.1.1. Users need to seek authorization from the IT department for any issues relating to BYOD.

3.1.2. The BYOD administrator is responsible for authorization, and in any situation that the BYOD administrator is unavailable; the user can seek the IT manager.

3.2 Authentication:

3.2.1. The BYOD administrator is responsible for authenticating users, and in any situation that the BYOD administrator is unavailable; the user can seek the IT manager.

3.3 Communication:

3.3.1. For any communication related setup or connection; users must make contact with the BYOD administrator.

3.4 Security:

3.4.1 Access control:

3.4.1.1. Users should always ensure the protection of the municipal information at all times, anywhere they are.

3.4.1.2. The municipal reserves the right to enable and disable certain applications on the mobile devices in order to ensure optimal security.

3.4.2 Information separation:

3.4.2.1. The municipal information to be stored and accessed in the BYOD devices will be separated from the user's personal information.

3.4.3 Support:

3.4.3.1. The municipality is committed to a seamless use of BYOD. Therefore, the municipality offers various supports for users. Below are the types of support available:

- **Technical support** - For any technical issues associated with the mobile devices could be handled by the IT department. Users must make communicate via email to the IT manager or BYOD administrator to acquire assistance.
- **In-house support** – For any other mobile device issues, users can contact in-house support at their designated municipality.
- **Self-help** – Users can make use of online websites, posters, emails and other self-help material that is made available for all users.
- **Online support** – Online support is made available for users. Users can access the details for online support from the IT department or municipal email communiqué.

3.4.4 Reporting:

3.4.4.1. Users should report any changes that occur to the BYOD administrator. Issues to report include but are not limited to the following: Changing devices (upgrade), adding a new device, removing an old device, fraudulent incidents, lost devices and hacking incidents.

3.4.5 Updates:

3.4.5.1. Applications and software need to be regularly updated. There are two options offered by the municipality for updates:

- **Manual:** The IT department manually updates the applications and software. (The user is responsible for reporting to IT department when they are in need of a manual update, when an application or software expires before regular update intervals)
- **Automatic:** The IT department automatically updates the applications and software.

3.4.6 Monitoring:

3.4.6.1. There will be constant monitoring of logs, voice and data usage and every activity that is on the municipal network. Action will be taken on any misuse of the municipal network.

3.4.7 Device and Application Management/Security:

3.4.7.1. Each municipality should incorporate the appropriate technology for managing the security and applications of BYOD devices.

3.4.8 Compatibility Testing:

3.4.8.1. Compatibility testing should be implemented on BYOD devices.

Appendix E: IST- Africa presented and published

Governing Information Security Within the Context of “Bring Your Own Device in SMMEs”

Noluvuyo FANI¹, Rossouw VON SOLMS², Mariana GERBER³

*Nelson Mandela Metropolitan University,
University Way, Port Elizabeth, 6001, South Africa*

¹Tel: +27737754931, Email: s207068382@nmmu.ac.za

²Tel: +27415043607, Email: Rossouw.VonSolms@nmmu.ac.za

³Tel: +27415043705, Email: Mariana.Gerber@nmmu.ac.za

Abstract: Information is a critical important asset; and it will always influence the way an organization conducts its business processes. Like any important business asset in an organization, there must be the assurance that the business information and related technologies are both protected and secure. Like any era in the advancement of technology, there is a new phenomenon that has grown in status: “Bring Your Own Device (BYOD)”. BYOD combines the official organizational devices required to function at work, together with the personal mobile device. There are many benefits to implementing BYOD; but because many risks are associated; and since BYOD is a new phenomenon, it can be difficult for organizations to manage in a secure manner. Therefore, this paper will provide a basic guideline to Executive Management on how they can govern and manage the BYOD phenomenon in SMMEs in a responsible way.

Keywords: BYOD, SMMEs, mobile devices, information security, IT governance

1. Introduction

In order for employees to do business within an organization, they need information, whether it be for writing a report or calculating finances [1]. Therefore, this means that organizational tasks begin and end with information.

Information is thus an important organizational asset, without which the organization would fail in the operation of its functions. Information is an intangible asset that needs protection within the organization. There are various threats that can destroy this important information, if there is a lack of proper protection [2]. Tools such as antivirus packages, password encryption and suchlike, have been used to facilitate the protection of information [3]. Thus, this allows proper protection of the information against threats. Therefore, with the protection of the information, employees can access and process the information in security-controlled environments.

Historically, employee accessibility and the processing of information was conducted through a mainframe that later advanced to a desktop computer. An employee within the parameters of the organization would be able to complete the organizational tasks. The needs of organizations and employees through history have been continuously changing; and technology has been developing, in order to accommodate the different needs that organizations have [4].

The needs include a technology that would break the boundaries of doing tasks within the parameters of the organization. Organizations have been looking for technologies that allow ease-of-use for employees, minimal training for employees; but most importantly, technology is needed that reduces the costs. In summary; what is needed, is an innovative

technology; that provides the competitive edge. Technology has since adapted - with the development of mobile devices - which are inclusive of laptops, smartphones and suchlike [5].

Mobile devices allow for the “mobility” of being used within and outside organizational boundaries: to access emails, files and other information of the organization. Most recently, there is a new technological phenomenon for mobile devices and that is the emergence of ‘Bring Your Own Device’ (BYOD) [6].

‘Bring Your Own Device’ allows for ease-of-use for an employee; because the employee is familiar with using his/her own personal mobile device; and additionally, they would not need training on how to use the personal mobile device. This reduces the costs associated with the technology; because in most cases, the employee purchased the personal mobile device. The greatest benefit, is that an employee can access and store the important information of the organization [7]. Consequently, organizational tasks are completed in a single platform, via a mobile device.

The use of BYOD is not limited to how large or small an organization is. Large organizations and Small-Medium Micro Enterprises (SMMEs) are utilizing, or want to utilize, BYOD. As with any technology that has the opportunity to be beneficial to an organization, both large organizations and SMMEs may be weary of implementing BYOD; because it has some risks associated with it [8]. As a result, this paper will highlight the importance of information in an organization, and how it can be secured and protected. The paper will further go into the details of the development of communication in mobile devices, the phenomenon of BYOD, and how SMMEs are affected. Finally, best practices and risk factors for BYOD will be discussed – before presenting the guidelines for securing information in BYOD.

1.1 Information in Organizations

1.1.1 Information Asset

Information is intangible. This means, that there is no means of touching or measuring its size, or to view its value. Although that is the case, the intangible information is used to run most of the organizational processes in an organisation. Thus, this means that although the information’s value cannot be weighed or touched, it does not mean that the information is not valuable. Furthermore, information is the key to all organizations, as it is an important organizational asset [9].

As with any asset, intangible or not, an organization would need to protect the information. Some organizations may find this task difficult; but it is important to identify how the information is used, in order to conduct the organizational processes. This gives organizations an indication as to how the information should be secured and protected. Consequently, the confidentiality and integrity of the information must be adequately managed [10].

1.1.2 Securing Information

Information is accessible and processed with various assets. These include the software, the infrastructure, the hardware, the human operator and the network. Systems are put in place to secure and protect the availability, confidentiality and integrity of the organization’s assets. Systems like: password encryption and/or biometrics are needed to ensure that only authorized employees can access the organization and its information, in addition to backing-up facilities for lost or stolen information, etc. [11]. A survey of IT and security professionals reported that IT professionals cite 82% of lost or stolen information as the top ranking mobile security incident concern [12]. According to Hewlett-Packard 50% of employees using three or more mobile devices to complete business tasks cannot be viewed

or traced by the IT department [13]. This entails that the organizational information is susceptible to various risks and threats, as the BYOD devices are either “unknown”, lost or stolen. Thus, the protection and securing of information and other assets within the organization means that the assets would not be vulnerable to unauthorized, access or use [14].

Employees are the human asset of the organization; as they are valuable, since they process information authorized to them. As the human asset of the organization, authorized employees need to be aware of their role in protecting all the other assets of the organisation, when accessing the information. This can be accomplished through consistent education and awareness programs, and through policies and procedures. Once employees are fully aware, the monitoring of compliance can be enforced to allow for accountability, responsibility and the ongoing monitoring of these employees [15]. Thus, proper steps can be taken when there is an improper access or use of information; the employees are knowledgeable in regard to their responsibilities for the securing of such information.

Mobile devices are part of the organization; and they have played an important role in how such information would be communicated, utilized or accessed; thus, it is important to view how they should assist organizations in conducting their organization’s processes.

2. Development of Communication and Mobile Devices

During the 1960’s, the communication of information was made through computer and telephone networks. This was known as an era commonly associated with mainframes and expensive IT equipment [16]. The 1990’s saw the evolution of technology - with the era of ubiquitous computing (laptop, PCs etc.), Local Area Networks (LAN) etc. Technology in an organization could now be used to ensure timely completion of organizational processes, with a technological competitive edge, and the reduction of costs - while simultaneously improving production [17].

In this era, mobile devices were also being used as a means of communicating organizational information to the ubiquitous computing of employees working in the comfort of their own homes as telecommuters [18]. This evolution became the driving force for developing a means of technology that could fulfil the goal of an employee being able to communicate on their mobile device within and outside the boundaries of the organization. Most importantly, information sharing became possible through technology, with the reduced costs of IT and ease-of-use [19].

An attempt to reach this goal was with the development of wireless communication. It began with the generation of radio-frequency technology, and grew into third-generation (3G) wireless technology, which allowed wireless connectivity through a wide area of networks (WANs). The year 1998 saw the development of Bluetooth, where there was connectivity and communication of information between different mobile devices (laptops, mobile phones, computers etc.) over a short distance [20].

Real Wireless and Rethink Technology Research estimates that wireless communication suchlike Wi-Fi hotspots will increase from 14% to 72% by the year 2018 as shown in Figure 1. This can be achieved through the quality of experience (QoE) by “integrating Wi-Fi with cellular and wireline (landline or telephone wire) networks”. Consequently, this opens the lines of communication and information sharing for organizational processes including emails, files and suchlike between mobiles devices through the use of Wi-Fi.

Furthermore, organizations should be able to “afford” the flexibility and ease-of-use of personal mobile devices as an official device. This should further meet the goal of communication within and outside the organization’s boundaries [20]. Thus, it is clear that accessibility through mobile devices has grown considerably over the last few years, and will continue to grow.

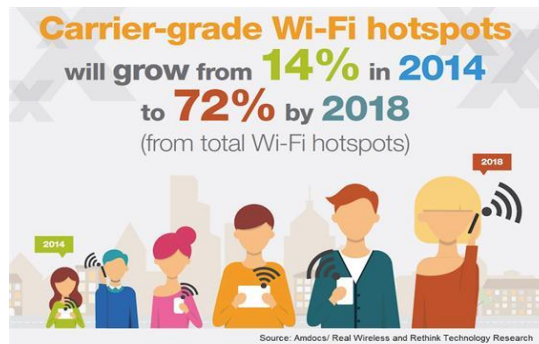


Figure 1: Wi-Fi Growth Estimation

The integration of personal mobile devices and official devices has resulted in the emergence of the phenomenon of ‘Bring Your Own Device’ (BYOD). Although, BYOD is new, and knowledge needs to be gained about it, this does not stop the growth and development of the BYOD phenomenon [21]

3. BYOD

Sheridan et al.[21], describe BYOD as *“the circumstance, in which users make their own personal devices available for company use; and the consumer devices enter the workplace”*. Furthermore, there are benefits to implementing BYOD for organizations since they would allow for the “dual-use” of a single device, where phrases like:

- “Anything”: means that the personal and organization’s mobile device use goes beyond work-related tasks;
- “Anywhere”: means that mobile device can be connected through wireless networks and hotspots, or even the internet;
- “Anytime”: mobile device use by employees, whether they are at home or on the premises of the organization.

With the benefits of BYOD listed above, BYOD will be appealing to organizations both large and small. However, as with any technology, there are some security risks and threats that are associated with BYOD. Cyber-threats, malware, malicious attacks and phishing are some of the biggest threats found with the use of emails and social platforms on mobile devices.

An Australian password use and management report by the Centre for Internet Safety found that 36% of the average Australian remains logged-in on their online accounts on their mobile devices; and 60% use the same password for more than one account. An employee implementing BYOD does not only make the organization’s important information susceptible to cyber-threats’ but this risk would also affect the individual employees’ personal and confidential information stored in their mobile device [22].

Yang, Vlas, Yang, and Vlas [23] stated that employees’ who own devices, like laptops, smartphones, tablets, and PDAs, are typically perceived as being less secure than devices used by the employer; but big companies have already integrated certain regulations; while others are currently implementing rules to deal with the possible threats [23].

A paper written by H. Twinomurizi and T. Mawela [24] reported that employees believe that using their personal mobile device at work is not an option; and they would use their device “with or without formal organizational BYOD programs” [24]. Hence, there is popular demand for the implementation of BYOD - with its advantages and disadvantages. But just where does the responsibility and management of information security lie?

4. SMMEs

BYOD is a phenomenon that has been associated with opportunities and risks. Organizations, like SMMEs are more susceptible to the risks of BYOD; as they may have limited security resources or lack of awareness [25]. This includes the lack of Business Continuity Plans, when there are system failures, or inexperienced IT staff responsible for the organizations network, software and IT infrastructure. Employees are known to connect to unsafe Wi-Fi hotspots that allow attackers to view employee passwords and other personal information and log-ins; and the organisation's information stored in portable devices, such as laptops being lost [25]. The information in SMMEs then becomes a target for attackers.

Literature pertains to various strategies, frameworks and guidelines for the management of BYOD. Zahadat, Blessner, Blackburn, and Olson [26] formulated a "BYOD Security Framework" that is divided into seven phases for managing BYOD [26]. An alternative solution is that of the "BYOD framework" that seeks assistance from the ISO/IEC 27000-series and strategic management for the governance of BYOD [27]. Although there are different BYOD management solutions currently in literature, there is a lack of solutions that govern the risks associated to BYOD within an SMME context. Therefore, with all the risks currently in SMMEs, if an SMME wants to implement BYOD, there should be effective management and control for BYOD.

5. Information Security Best Practices

Information in an organization needs consistent protection from any security risks, threats and attacks. There are policies, procedures and strategies that can assist an organization in their task of the protection of the information. This section will go into the discussion on the three best practices related to information security, which are: the King III report (governance principles); COBIT (management practices); and ISO 27002 (information security controls).

Executive management are responsible for the governing and managing of the organization's important information and IT resources. When there is a lack of proper governance of the information and IT resources in the organisation, the executive management is accountable. The King III report provides seven governance principles that can be applied by the executive managers who are responsible and accountable for the governance.

Chapter 5 of the King III report clearly states how executive management can protect and govern IT. When there is an asset involved, there are risks that can be encountered. Therefore, there is a need for risk management. Chapter 4 of the King III report contains recommendations for the executive management for the governing and managing of such risks. Thus, executive management should utilise and adhere to the King III report, in order to maintain the sustainability of the organisation [28].

Another best practice that can be used by executive management includes the Control Objectives for Information and related Technology (COBIT). It is an *"internationally accepted IT governance control framework for the adoption by enterprises for the day-to-day use by business managers, IT professionals etc."*

COBIT has the aim of aligning the IT and business of the organization [29]. COBIT 5 covers the IT and organizational related tools for executive management to effectively govern and manage the organization. The domain of interest in this research is that of the Delivery, Service and Support (DSS) which encompasses six processes, specifically DSS05, Manage Security Services. The DSS domain gives recommendations for the effective management of the execution and support of IT systems. Process DSS05 (Manage Security Services) further states how an organization can maintain information with the use

of an information security policy. Process DSS05 consists of seven management practices to implement managed security [30].

To further deliver value and manage the information security, executive management can utilise the best practice known as ISO 27002. ISO 27002 consists of control objectives and controls that can assist when organizations want to identify potential information-related risks by implementing risk assessment. Furthermore, in the ISO 27002 standard, within category 6.2 “Mobile device and teleworking”, there is control 6.2.1 “Mobile device policy” that provides guidelines for ensuring that the mobile devices are secure from risks. [31]. Although there is the “Mobile device and teleworking” category within the ISO 27002 standard, the entry refers to mobile devices but BYOD is implied and not specifically mentioned. Once the risks are identified, they can be treated. The information security controls allow organizations to compare themselves against the ISO standard through a formal certification, and view whether they complied with the ISO standard.

Therefore, when organizations are certified and complied, there is the assurance of the control and management of the information security [32]. Thus, best practices do play an important role in safeguarding valuable information assets. Also King III, COBIT and ISO 27002 can be utilised seamlessly together.

6. Risk Factors Relating to BYOD and SMMEs

Employees want to stay connected anywhere, anytime and without any constraints and limitations. The way in which they want to stay connected, is on their hi-tech personal devices, which would include laptops, iPads, and smartphones. Trend Micro Inc. have reported in their survey findings that 74% of IT enterprises are succumbing to the needs of employees, by allowing them to stay connected, anywhere, anytime on their personal devices [33]. Although, this is so, these employees should have restrictions and limitations when using BYOD.

A survey report done by Ghosh and Rai [34], found that 21% of organizations preferred to issue an official mobile device to employees; but would hold the employees responsible for the management of the device [34]. Thus, when organizations allow users to manage their official mobile device, who would then be responsible for the security risks and unauthorised access to information?

The Norton report for the year 2013, found that 26% of “smartphone users have mobile security software with advanced protection”. What is alarming is that; 36% of respondents, who make use of BYOD, state that their company has NO BYOD policy [35]. Therefore, this means that although organizations implement BYOD, the effort needed to govern and manage BYOD is still lacking.

A study conducted on SMMEs in the Twente region in the Netherlands, found that 38% of SMMEs see IT-related security incidents damaging and the biggest risk to their IT infrastructure. It was found that, although SMMEs reported minimal security incidents, it was probable that the risks were masked by hackers who had broken into the IT infrastructure [36]. If this is the case, SMMEs who implement BYOD may face some of the following risk factors with their employees. The risk factors below further indicate their association with the information security best practices [37]:

Risk factor 1: *Lack of control on what the employees may access on their personal mobile devices.* Executive management provides direction to the organization, and must ensure that policies are set, and that employees comply with the policies set (King III report). A BYOD policy for information security should state, amongst other issues, access control to IT services and applications. COBIT 5 consists of DSS05 Manage Security Services domain that states how the BYOD policy for information security needs to be implemented by employees, how this can be maintained and used.

When the employees use their personal mobile device for unrelated work use, there are risks to the protection of the organizations information. Malware, cyber-attacks etc. can breach the security measures put in place by the organization. If there are any risks identified, they must be managed and controlled [32].

Risk factor 2: *Lack of control on the number of personal mobile devices an employee can own.* When a BYOD policy is being set, the executive management should lead the organization in effectively implementing the policy (King III report). This includes ensuring that the BYOD policy clearly states who can use their personal mobile device for BYOD; as well as how many personal mobile devices each employee can use for BYOD etc. [38]. When there is control over the number of devices an employee can use, there can be monitoring; and access control can be implemented on the BYOD devices [32].

Risk factor 3: *Managing the data integrity and confidentiality of the organizational information by stating who will access which information.* The King III report states how executive management can protect the important information and thereby maintain the integrity and confidentiality of the information asset. Guidelines for the implementation of the Governance of Enterprise IT (GEIT) are made available for the executive management in COBIT. Furthermore, ISO 27002 provides the controls for securing, monitoring and managing of such an information asset.

Risk factor 4: *Organizational information lost, or the confidentiality or integrity gets compromised, when the mobile device used for BYOD is lost or left unattended.* The King III report states that it is the responsibility of the executive management to govern valuable company information. Therefore, to manage the risk and protect and secure the information when a mobile device is lost or stolen, COBIT can be used as a guide. Proper risk management would need to be implemented; and ISO 27002 can be used to confirm that risk assessment has been performed; or the executive management must be held accountable.

Risk factor 5: *Inability of proper risk management, as BYOD is continuously evolving and the computing-related changes can be challenging for SMMEs.* Chapter 4 of the King III report is dedicated to giving recommendations on the governance of risk management. COBIT and ISO 27002 highlight the importance of managing risks.

The challenges of BYOD on SMMEs would indeed need guidelines on how the SMMEs intend to manage and govern the phenomenon of BYOD; if they want to secure the information within the organization. With this in mind, executive management can manage the organization by making use of the principles (King III report), practices (COBIT) and controls (ISO 27002) in place. Although, not all the principles, practices and controls are applicable to every organization, they can guide executive management in SMMEs through the proper management and governance of BYOD. However, with the everyday challenges that SMMEs have, how would they even begin to formulate the guidelines?

7. Guidelines Towards Securing Information in BYOD

The securing of the information-related assets in the SMME will need directives from Executive management. A policy is one of the tools that can be used. The policy would include all the guidelines on how the SMMEs need to secure the information, when implementing BYOD - bearing in mind the resources in the SMME [36]. Therefore, when there is a guideline required for BYOD, SMMEs can manage it.

The guidelines provided in this paper are based on aspects from existing guidelines and solutions in literature, a mind map and focus group. Thus, a policy for BYOD in SMMEs could include the following guiding factors that state how the policy can be implemented by using the fore-mentioned information security best practices as a guide:

Risk factor 1: Executive management will accept the responsibility of providing direction for the BYOD policy. Giving direction would require the executive management

to state the vision they have for the BYOD policy, and seeing that vision materialise by directing the other levels of management within the organisation. The policy should clearly specify who is allowed to make use of BYOD, according to the job titles of the employees. Once identified, the employee should agree to the terms for using BYOD [28]. When there is an agreement in place, domain DSS05 will provide recommendations for sufficient management of the policy. The management of the policy includes the organization setting up controls to authenticate and identify the users [38]. Measures to authenticate and identify users, should allow verification and monitoring. There could be a firewall application, which can monitor the organization's network and restrict any traffic to certain applications. When the BYOD device is monitored, there can be activity logs to view employee activities – and to ascertain whether these activities are part of the BYOD policy agreement, or not [32].

Risk factor 2: The executive management should lead, by appointing a Chief Information Officer (CIO), or someone responsible, who would be responsible for the management of IT, including BYOD [28]. Thus, the CIO would have the experience and knowledge to provide insight on how many BYOD devices an employee should be allowed to have. When the number of devices attached to an employee is established, this would allow for technologies like cryptography to be implemented in the BYOD device [32]. Consequently, control could be established, according to the BYOD device.

Risk factor 3: The confidentiality and integrity of the information is important, as information is a core asset within the organization. The executive management should ensure the confidentiality, integrity and governance of the information [28]. The GEIT of the information should not be limited to the information; but also to the technology of BYOD.

The mobile devices used for BYOD should have systems in place to block and prevent any hacking, malware, viruses, phishing etc. [38]. An organization can implement a Blacklist and Whitelist approach, where the Blacklist contains the malicious applications and the Whitelist contains the non-malicious applications. With organizations having to face issues like social engineering, it is important to take the precautions needed to effectively ensure the protection of information [32]. Therefore, with the support of the executive management and recommendations, it should be possible to protect the information assets of the organization.

Risk factor 4: There should be resources in the organization for when the information on the BYOD mobile device is hacked, stolen or the device is lost [28]. These should include mobile device management (MDM), by means of remote wiping, or locking of information, encryption of information, and back-up facilities [38]. Constant risk assessments would need to be made for the information that is stored on the BYOD devices. Although, the wiping, locking and backing-up of information on the BYOD devices is the responsibility of the IT department, the executive management would still need to take due care and remain resilient in the governing of information security .

Risk factor 5: The executive management does not only lead and direct the organization; but they also need to control it as well. Control means that there needs to be compliance measured against the BYOD policy set. Compliance is measured at the middle and lower management levels [28]. Once compliance is measured, there needs to be a report of compliance to the executive management [38]. Compliance with the BYOD policy should be monitored consistently, especially the compliance of employees. There should be a risk-management program, which could update and maintain the policy, while monitoring any potential risks. When there is a lack of compliance, there should be actions taken [32]. Therefore, when there is constant monitoring and auditing of compliance, the risks of BYOD are minimized.

Table below summarises five risk factors that can be used in a SMME BYOD policy.

Factors	King III							COBIT						ISO 27002									
	IT governance	IT alignment	IT responsibility	IT monitoring	Risk management	Asset management	Committees	Manage operations (DSS05.01)	Manage service requests and incidents(DSS05.02)	Manage problems (DSS05.03)	Manage continuity (DSS05.04)	Manage security services (DSS05.05)	Manage business process controls (DSS05.06)	Security Policy	Organizing Information Security	Asset Management	Communication and Operations Management	Access Control	Risk Assessment and Treatment	Information systems acquisition, development and maintenance	Information Security Incident Management	Compliance	
	Principles							Management practices						Security control clauses									
Risk factor 1: Access control over mobile device applications	Executive management directs and provides the vision for the BYOD policy							Management of the IT services transcribed for BYOD						Controlling access to applications									
	x		x					x	x			x	x	x	x		x	x		x	x	x	
Risk factor 2: Control over the number of devices per employee	Appointment of a CIO for the management of BYOD and IT							Management of IT allows management of the number of BYOD devices						Management allows control per device									
	x		x			x	x			x				x		x						x	
Risk factor 3: Integrity and confidentiality of information	Governance of integrity and confidentiality of information							GEIT of information						Controls to protect the information									
	x	x		x					x	x	x	x		x			x	x	x		x	x	
Risk factor 4: Information on lost or stolen mobile device	Governing of lost or stolen information							Security of information on BYOD devices						Risk assessment									
	x			x	x	x		x	x	x	x	x		x		x	x	x		x	x	x	
Risk factor 5: Risk management and Compliance	Compliance reporting							Risk management program						Auditing of the Risk management program									
					x		x	x				x		x			x		x			x	x

8. Conclusion

With the threats and risks that affect the information assets, the organization should harbour a culture of protecting their information at every avenue [39]. SMMEs are not exempted from the threats and risks, and should take precautionary measures. This paper discussed the importance of information in an organization, and how it can be secured and protected. Furthermore, the development of communication in mobile devices, the phenomenon of BYOD, and how SMMEs are affected was discussed. Identified existing guidelines and solutions depicted in literature for BYOD were studied, and a mind map illustration and

focus group were executed during the analysis. Findings from the analysis revealed that there is a lack of governance and management of BYOD in SMMEs. Therefore, best practices and risk factors for BYOD were discussed in this paper, followed by the proposed guidelines for securing information in BYOD.

The proposed guidelines for securing information in BYOD state how a BYOD policy can be implemented by using the fore-mentioned information security best practices as a guide. With the BYOD phenomenon, SMMEs can make use of the five risk factors stated above; so that they can effectively address the threats and risks involved. Therefore, SMMEs could relish the benefits of BYOD. Future work could consist of the development of a BYOD policy and other forms of guidelines for the governance and management of BYOD, particularly in SMMEs.

Acknowledgements

The authors hereby acknowledge the financial assistance of the Council for Scientific and Industrial Research (CSIR) and Nelson Mandela Metropolitan University (NMMU) towards this research. Opinions expressed and conclusions arrived at, are those of the authors and not necessarily that of the CSIR or NMMU.

References

- [1] M. Broadbent, "The phenomenon of knowledge management : What does it mean to the information profession ?," *Inf. Outlook*, vol. 2, no. 5, pp. 23–26,28–30,32, 34–36, 1998.
- [2] R. G. Brody, E. Mulig, and V. Kimball, "Phishing, pharming and identity theft," *Acad. Account. Financ. Stud. J.*, vol. 11, no. 3, pp. 43–56, 2007.
- [3] T. Caldwell, "Data loss prevention - Not yet a cure," *Comput. Fraud Secur.*, vol. 2011, no. 9, pp. 5–9, 2011.
- [4] A. a. Shaikh and H. Karjaluoto, "Making the most of information technology & systems usage: A literature review, framework and future research agenda," *Comput. Human Behav.*, vol. 49, pp. 541–566, 2015.
- [5] B. Andrew, "TCO & Security of Enterprise Grade Mobility," 2012.
- [6] G. Thomson, "BYOD: Enabling the chaos," *Netw. Secur.*, vol. 2012, no. 2, pp. 5–8, 2012.
- [7] A. Weeger and H. Gewald, "Factors Influencing Future Employees Decision-Making to Participate in a BYOD Program: Does Risk Matter?," 2014, pp. 0–14.
- [8] *The Role of IS Assurance & Security Management*, vol. 1. 2013.
- [9] D. Moody and P. Walsh, "Measuring The Value Of Information: An Asset Valuation Approach," *Seventh Eur. Conf. Inf. Syst.*, pp. 1–17, 1999.
- [10] T. Coulson, J. Zhu, T. Coulson, and J. Zhu, "The Price of Security : The Challenge of Measuring Business Value Investments in Securing Information Systems Investments in Securing Information Systems," vol. 5, no. 4, 2005.
- [11] P. Weill and M. Vitale, "What IT infrastructure capabilities are needed to implement e-business models," *MIS Q. Exec.*, vol. 1, no. 1, pp. 17–34, 2002.
- [12] "THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY : A survey of IT and security professionals," 2014.
- [13] T. Noda, "Solving BYOD issues a must says HP," 2013. [Online]. Available: <http://www.philstar.com/business/2013/03/16/920437/solving-byod-issues-must-says-hp>. [Accessed: 30-Mar-2016].
- [14] ISACA, "Data Leak Prevention," no. September, pp. 1–14, 2010.
- [15] T. C. Redman, *Data Driven: Profiting from Your Most Important Business Asset*. United States of America: Harvard Business Press, 2008.
- [16] U. H. Rao and U. Nayak, "The InfoSec Handbook An Introduction to Information Security," in *Apress*, 2014.
- [17] M. Attaran, "Exploring the relationship between information technology and business process reengineering," *Inf. Manag.*, vol. 41, no. 5, pp. 585–596, 2004.
- [18] K. Lister and T. Harnish, "The State of Telework in the U . S .," *Network*, no. June, pp. 1–27, 2011.
- [19] G. Widen-Wulff, "Explaining knowledge sharing in organizations through the dimensions of social capital," *J. Inf. Sci.*, vol. 30, no. 5, pp. 448–458, 2004.
- [20] C. Bisdikian, "An overview of the Bluetooth wireless technology," *IEEE Commun. Mag.*, vol. 39, no.

- 12, pp. 86–94, 2001.
- [21] J. Sheridan, R. Ballagas, and M. Rohs, “BYOD: bring your own device,” *Procedia Technol.*, vol. 9, pp. 43–53, 2004.
 - [22] D. Dang-pham and S. Pittayachawan, “Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university : A Protection Motivation Theory approach,” *Comput. Secur.*, vol. 48, pp. 281–297, 2014.
 - [23] T. A. Yang, R. Vlas, A. Yang, and C. Vlas, “Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior,” *Proc. - Soc. 2013*, pp. 411–416, 2013.
 - [24] H. Twinomurizi and T. Mawela, “Employee perceptions of BYOD in South Africa : Employers are turning a blind eye ?,” pp. 126–131, 2014.
 - [25] S. (WatchGuard T. Pinzon, “Top 10 Threats to SME Data Security (and what to do about them),” *October*, pp. 1–3, 2008.
 - [26] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, “BYOD security engineering: a framework & its analysis,” *Comput. Secur.*, vol. 55, pp. 81–99, 2015.
 - [27] M. Brodin, “Management issues for Bring Your Own Device,” 2015.
 - [28] K. M. E., “for South Africa – 2009 (King iii) - King committee on governance,” no. King iii, 2009.
 - [29] B. K. Jensen, S. Baar, G. Assistant, and L. Rock, “Making Security Policies Memorable : the First Line of Defense,” vol. 4, no. 2, pp. 28–36, 2014.
 - [30] *COBIT 5: Enabling Processes*. 2012.
 - [31] *SANS 27002 : 2014 SOUTH AFRICAN NATIONAL STANDARD Information technology — Security techniques — Code of practice for information security controls*. 2014.
 - [32] I. Standard, “Information technology — Security techniques — Code of practice for information security management,” 2005.
 - [33] I. Yevseyeva, C. Morisset, J. Turland, L. Coventry, and T. Groß, “Consumerisation of IT : Mitigating risky user actions and improving productivity with nudging,” *Procedia Technol.*, vol. 16, pp. 508–517, 2014.
 - [34] A. Ghosh and P. K. G. S. Rai, “Bring Your Own Device (Byod): Security Risks and Mitigating Strategies,” *J. Glob. Res. Comput. Sci.*, vol. 4, no. 4, pp. 62–70, 2013.
 - [35] “2013 Norton Report,” 2013. .
 - [36] B. Van Ommen, “IT Security in SMEs: Necessary or Irrelevant?,” 2014.
 - [37] K. Madzima, M. Moyo, and H. Abdullah, “Is Bring Your Own Device an institutional information security risk for small-scale business organisations ?,” 2014.
 - [38] *COBIT 5: Implementation*. United States of America.
 - [39] S. Allam and S. Flowerday, “An adaptation of the awareness boundary model towards smartphone security,” *2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf.*, 2011.

Appendix F: ISSA presented and published

A framework towards governing “Bring Your Own Device in SMMEs”

Noluvuyo Fani, Rossouw von Solms and Mariana Gerber

Center for Research in Information and Cyber Security

NMMU

NMMU, University Way, Port Elizabeth, 6001, South Africa.

s207068382@nmmu.ac.za, rossouw.vonsolms@nmmu.ac.za , mariana.gerber@nmmu.ac.za

Abstract — Information is a critically important asset that has been used for decades within organizations. Like any asset, there are threats to the information that impact processes such as; email retrieval and access to organizational system services. As a consequence of the threats, attention to the security of the information is important. Technology is utilized to secure information and the cost affiliated to the technology can be dire. As technology evolves with each transitory decade, there are different phenomenon's that attempt to process and secure organizational information whilst reducing costs. The evolution of technology has developed a new phenomenon called “Bring Your Own Device” (BYOD). BYOD is a phenomenon that allows employees to use their own personal mobile device to complete organizational tasks. The adoption of BYOD expands from large organizations to small, medium and micro enterprises (SMMEs). With the adoption of BYOD there are benefits and more significantly risks associated to BYOD. Therefore, this paper will discuss the SMME context and its challenges towards the governance of BYOD. In addition, there will be a discussion on how organizations can govern BYOD in an SMME context by considering the existing BYOD approaches and provide an approach suitable for SMMEs. Furthermore, the suitable BYOD approach for an SMME context will further be evaluated and compared against the existing BYOD approaches that were identified. The research process of the study is conducted within the design-oriented research paradigm utilizing a cyclic approach.

Keywords- BYOD, SMMEs, mobile devices, information

Security.

I. INTRODUCTION

There are various assets that are composed within an organization. Assets such as; humans, information and capital are composed within the organization. An asset can be categorized as tangible or intangible. An intangible asset is an asset that *cannot* be seen or touched (e.g. patents) and a tangible asset *can* be seen and touched (e.g. computer) [1]. There is a value attached to each asset whether it is tangible or intangible, and therefore, assets are important within an organization and should be protected.

Information is a valuable intangible asset. It can be defined as “data with attributes of relevance and purpose. It is usually in the format of a document or visual and/or audible message.

Additionally, information should convey a message that must be understood” [2]. Organizations utilize information to complete their daily tasks as information is a universal form of communication. The communication of information will be through sources of; emails, telephonic, paper-based documentation etc. The information communicated will be specific to each organization and might contain some “secrets” of the organization [3]. Due to the uniqueness pertaining to the organizational information, organizations should implement security mechanisms that should safeguard the confidentiality, integrity and availability (CIA) of the information [4].

The security mechanisms implemented will reduce the likelihood of breaches to the CIA of information and the information remains intact [3]. The technological tools attained to process and secure information have changed and adapted to the changes and needs of organizations. Organizations prefer technology that allows an ease of use and accessibility while maintaining or reducing costs. Technology has developed to a rapid extent of bringing forth a phenomenon referred as “Bring Your Own Device” (BYOD) [5]. BYOD is an exciting development, which has caused an alteration in the way business is conducted and is affiliated with many benefits. However, with any technology, there are risks associated with BYOD.

A. BYOD phenomenon

BYOD is an acronym for “Bring Your Own Device” and can also be referred to as the *Consumerization of Information Technology*. BYOD can be defined as “the practice of allowing employees to bring to the workplace their own mobile devices that are capable of connecting to the organizational network.” [6]. The dual-use of a mobile device for personal and organizational purposes has offered the benefits of:

- **Accessibility** – Accessibility to organizational resources via the organizational network, allowing employees to work “anytime” and “anywhere”.
- **Increased Productivity and Innovation** – Minimal training is required due to the familiarity with the mobile device, thus, there is increased production and innovation.
- **Cost-Savings** - BYOD can assist in the reduction of costs towards organizational expenses as the device is purchased and owned by the employee [7].

The benefits affiliated with BYOD have allowed BYOD to gain momentum with both organizations and employees. Employee demand for the implementation of BYOD leaves the organization with minimal choice but to adapt to the changing environment [8]. With the benefits and adoption of BYOD from both large organizations and SMMEs, organizations should remain aware of the risks of implementing BYOD, as the confidential organizational information is accessed through the BYOD devices. The risks of implementing BYOD ranges from; data leakage, lost devices and hacking [9]. The next subsection discusses BYOD in an SMME environment.

B. BYOD in an SMME

SMMEs are encompassed by limitations in their budgets and resources. The benefits of the implementation of BYOD in an SMME could reduce the budgets and costs affiliated to the resources. This is due to circumstances such as the cost affiliated with the purchase of the BYOD devices is handled by the employee [10].

When an SMME implements BYOD limited budgets and resources should not be the only issue fixated on, but every aspect affiliated with BYOD must be taken into account. With this in mind, caution must be applied by the SMMEs as they can become easily susceptible to the risks associated with BYOD. There are BYOD initiatives such as; strategies, recommendations and frameworks outlined in literature. Before embracing these BYOD initiatives, SMMEs should understand their particular requirements and what is appropriate in their environment.

C. Requirements for BYOD in SMMEs

According to the National Small Business Amended Act No. 102 of 2004, a SMME definition is “a separate and distinct business entity, which is managed by one or more owner(s), which predominantly conducts its business in any sector and/or subsector of the national economy”. The SMME is all-encompassing of requirements such as; scalability, utility, efficacy and quality. Table 1 below provides a brief description of the allocated SMME categories [11]:

Table 1: Categories and descriptions of SMMEs[11]

Categories	Description
Survivalist enterprises	Operates in the informal sector of the economy. Minimal training or asset investments. Therefore, resulting in a lack of business growth.
Micro enterprises	One to five employees, usually the owner and family. An informal enterprise with no license, formal business infrastructure. Basic business skills and training.
Very small enterprise	Middle class economy. 10 paid employees or less Consists of self-employed artisans (electricians) and other pro.
Small enterprise	Approximately 100 employees. Registered, fixed business premises. Consists of complex management structure or managed by a single owner.
Medium enterprise	Owner managed and approximately 200 employees. Operates from fixed infrastructure with all formal necessary necessities for business.

The small stature and limited resources of SMMEs makes SMMEs vulnerable to weaknesses to their information. It is common that incidents of breaches to the SMMEs network and other resources develop. The pressure of the sustainability and the maintenance of existing SMME resources provides difficulties in monitoring other factors such as information security. The phenomenon of BYOD provides a competitive edge for any organization but with the strains and limitations found in SMMEs, the adoption of BYOD may be a hindrance instead of a competitive advantage. [12].

With the harsh reality of the limitations in SMMEs, there is a need for a solution that will cater for the desire of BYOD in an SMME environment. There are requirements that have to be taken into account when the BYOD solution is formulated. The requirements for BYOD solution in SMMEs should cater for the following:

- **Scalability** – Solution scalable for an SMME environment.
- **Utility** – Solution is usable in an SMME environment.
- **Efficacy** - Solution is efficient and developed with the SMME environment in mind.
- **Quality** – The solution formulated should provide value in an SMME environment.

This concludes that with the requirements for BYOD in SMMEs taken in context, an appropriate solution for the governance of BYOD can be devised. However, before formulation of the solution, it is vital to also consider the protection of the information within SMMEs as information is an asset in an organization regardless of organizational stature and limitations.

D. Information security characteristics of BYOD

Before the phenomenon of BYOD, organizations provided employees organizational mobile devices. With the phenomenon of BYOD, devices have the dual use of being used as a personal and organizational devices. As a consequence, employees have the advantage of accessibility to personal applications and services [13]. The security of the organizational information can be compromised when dealt with unknown applications and services entering the organizational network.

The IT department can only manage a certain degree of security on accessibility to personal applications and services. Therefore, employees within an organization should be made aware of their role in the security of organizational information. [6]. A foundation of characteristics for a suitable solution should be compiled as the initial phase for governing BYOD. Below is a list of eight BYOD characteristics identified from literature that an organization should follow:

BYOD Characteristics:

C1: There must be risk identification:

- “BYOD is an institutionalised security risk which small scale organizations need to assess and

evaluate before blindly embracing the practice” [6].

- “There are many potential risks and threats to confidential information resources and assets in organizations use BYOD devices” [7].

C2: There must be security requirements stipulated for BYOD:

- “The main goals of information security are confidentiality, integrity and availability” [3].
- “Legal and liability issues should be considered and stated in the BYOD policy” [14].

C3: The organizational context must be considered:

- “Uncontrolled environments present more dynamic risks within the specific context and circumstances of that environment” [15].
- “Organizations require accurate and reliable information because they communicate and manage substantial information resources” [7].

C4: There must be a BYOD device analysis:

- “BYOD consists of the use of personal devices. Only the definition does not state which devices it concerns” [16].
- “Devices should be registered for participation in the BYOD program, officially approved for use, and provisioned with required security settings” [5].

C5: The organization must take into context the employee role:

- “Users of mobile devices need to be aware of threats the mobile device threats and have competent skills to secure their devices” [17].
- “Users should be educated as they perform their daily activities, with frequent policy reminders that are non-intrusive and relevant to their current task” [19].

C6: There must be IT administration within the organization:

- “Organizations BYOD should realize the impact BYOD can have on technical support” [16].
- “It is crucial for organizations to employ a proper security model for mobile devices as security challenges will increase in organizations” [20].

C7: There must be a BYOD policy:

- “Policies are a good starting points for gaining control on an enterprise as they provide guidelines for BYOD adoption” [6].
- “The policy should provide clarity on how devices will be used and how IT can meet those needs” [21].

C8: An organization must have compliance:

- “A BYOD policy is likely to improve compliance by educating employees the risks associated with their devices” [6]. “Violation of the policy should have severe punishment” [22].
- “Companies must re-evaluate BYOD compliance” [23].

Once the BYOD characteristics are met, a solution can be formulated. In order for organizations to manage the demands of implementing BYOD, there are frameworks that have been formulated in literature. The upcoming section will present an analysis of some of the existing frameworks for managing BYOD.

II. EXISTING FRAMEWORKS FOR BYOD

There are many factors that dictate the approach in the formulation of a BYOD framework. As a result, the formulated frameworks for BYOD are specific to each environment or organization. In this paper, there are four frameworks that are considered for analysis as the existing formulated BYOD frameworks. The objective of the frameworks is the governance and management of BYOD. In this section, an outline of each framework will be provided and the distinction between each framework should be apparent. Subsequently, there will be a tabulated mapping of the BYOD characteristics mentioned earlier (Section I) and the identified frameworks. The objective of the mapping is to analyze whether the identified frameworks meet the requirements stipulated in the BYOD characteristics and if they cater for an SMME environment.

A. BYOD Security Framework

The first framework identified is the BYOD security framework [5]. This framework is divided into seven phases for managing BYOD. A brief description of each phase is as follows:

- **Plan:** Understand the context of the business. Identify the relevant users and resources they access.
- **Identify:** Devices are registered, approved, and provided with the appropriate security.
- **Protect:** The information held within the devices requires protection.
- **Detect:** The organization should prevent, or respond to and recover from, intentional or unintentional different threat events identified.
- **Respond:** The organization should respond to identified threats.
- **Recover:** The organization must be able to fully recover from the event.
- **Assess and Monitor:** An organization should assess and monitor the value and competence of the BYOD security program [5].

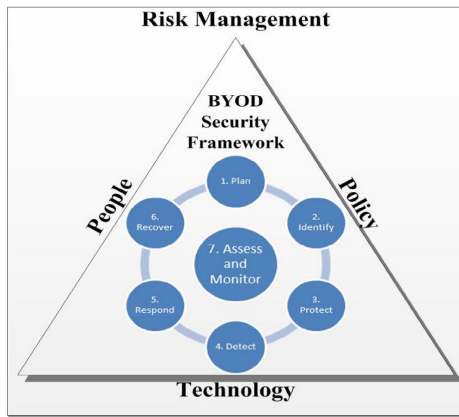


Figure 1: BYOD Security Framework [5]

Figure 1 illustrates the BYOD Security Framework. In illustration, the seven phases are encompassed by the three pillars of people, technology and policy. The purpose of the framework is to provide a foundation for a BYOD security program. The framework can be constantly amended. Furthermore, the BYOD Security Framework is formulated to form part of the risk management framework [5].

B. BYOD framework for a management system

The BYOD framework formulated governs BYOD by seeking assistance from the ISO/IEC 27000-series and strategic management. There are three steps that are specified in the proposed framework. The three steps are visualized in Figure 2 and are concisely defined as follows:

- **Analysis:** The organisation determines the relevant issues affect overall strategy and information security.
- **Design:** More analyses is conducted and there is the development of strategies. Existing policies are updated.
- **Action:** The organization should perform a risk assessment. When the risk assessment is completed, the strategy can be implemented.

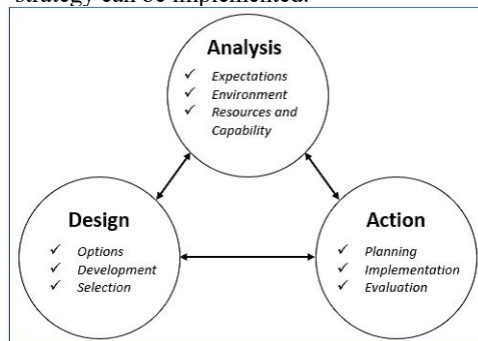


Figure 2: BYOD framework for a management system [24]

The framework provides a security and strategic way of thinking when an organization adopts BYOD [24].

C. BYOD privacy & culture governance framework

The third framework is the Bring Your Own Device implementation framework [25]. This framework maps the

organizational culture and privacy concerns within the organization. Once the mapping is complete, a policy is developed. The components prescribed in the framework are as follows:

- Determine the culture within the organization based on employee views.
- Delineate the characteristics that the organizational culture is based on.
- Identify the privacy concerns that would be applicable to the organization.
- Clearly define the individual concerns with regards to privacy.
- Conduct a privacy concern valuation based on employee's views. The assessment can assist in improving employee satisfaction.
- Develop a policy that takes account of the privacy concern assessment.
- Implement cloud management control, relate to the organizational culture.

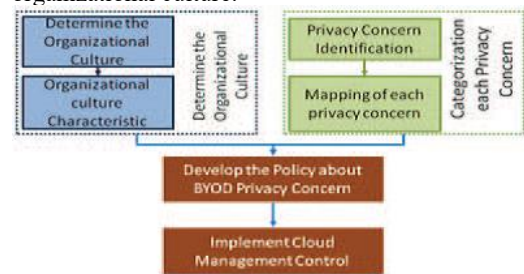


Figure 3: BYOD privacy & culture governance framework [25]

In Figure 3 the relationships of different components of the framework are diagramed. The purpose of the framework is to determine if organizations benefit in the implementation BYOD when organizational culture and cloud management control is adapted [25].

D. Enterprise and BYOD space BYOD Security Framework

The Enterprise and BYOD space BYOD Security Framework was formulated to protect the enterprise networks when BYOD is implemented. The represented framework is divided into two sides; the Enterprise side and the BYOD side. Below is brief description of each side:

- **Enterprise side:** includes the corporate resources and device management. The network access controls personal space and enterprise space.
- **BYOD side:** provides the functions that assist in separating corporate space, enforcing security policies, and the protection of corporate data [26].

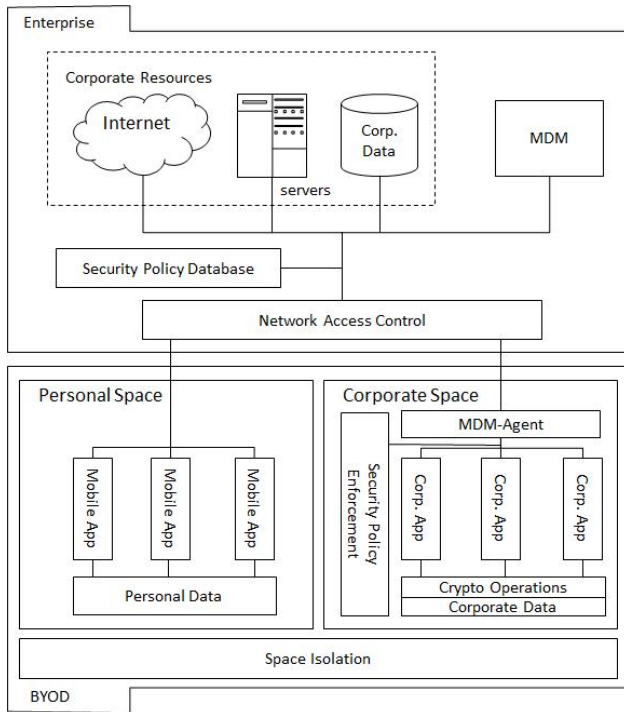


Figure 4: Enterprise and BYOD space BYOD Security Framework [26]

The enterprise and BYOD space BYOD Security Framework is presented in Figure 4. The framework provides protection to the organizational information by separating the network spaces that a BYOD user can access into enterprise space and BYOD space. This permits BYOD users to work in controlled and protected spaces. [26].

The four BYOD frameworks discussed above are similar in their intention of governing BYOD. Although, it is apparent that they are different in the way they are formulated and implemented. Eight characteristics were mentioned earlier and they provided a foundation for an appropriate BYOD solution. In Table 2 there is a mapping of the eight BYOD characteristics and the identified existing BYOD frameworks. The mapping analyses whether the identified frameworks meet the eight BYOD characteristics, and whether they cater for an SMME environment.

Table 2: Mapping of the BYOD characteristics and existing frameworks

Authors	C1	C2	C3	C4	C5	C6	C7	C8	SMME
[5]	✓	✓	✓	✓		✓			
[27]	✓	✓	✓		✓				
[25]					✓	✓	✓		
[26]		✓	✓	✓		✓	✓	✓	

From the analysis of the tabulated mapping, it is noticeable that although the frameworks meet some of the BYOD characteristics, but none of the identified BYOD frameworks cater for an SMME environment. Therefore, it would be difficult to assume that they would be appropriate to be

implemented in an SMME environment. BYOD high level management framework

The solution to the phenomenon of BYOD is not about developing numerous frameworks, but rather a framework that will allow the organization to reap the benefits of BYOD while taking into account the organizational environment and information protection. As small organizations, SMMEs are adopting and want to adopt BYOD. But in doing so, they encounter issues when it comes to a solution for the governance of BYOD. Thus, it is essential that a solution for governing BYOD in SMMEs is formulated.

III. BYOD MANAGEMENT SYSTEM (BYODMS)

The previous section demonstrated the four BYOD frameworks from literature. As evaluated, the frameworks lack in their diversity and alignment with the eight BYOD characteristics. Furthermore, they lack in addressing BYOD within an SMME environment. As a result of the challenges discussed, the proposed solution depicted in this section is that of the BYOD high level management framework. The BYOD high level management framework was formulated through a rigorous research process within the design-oriented research paradigm utilizing a cyclic approach. The first phase is an analysis phase where the problem is analysed, in the second phase is a design phase where solution is developed. The third phase is an evaluation phase which consists of the validation of the artifact against the specified objectives, methods etc. The fourth phase is the diffusion phase where the solution is finalised [28].

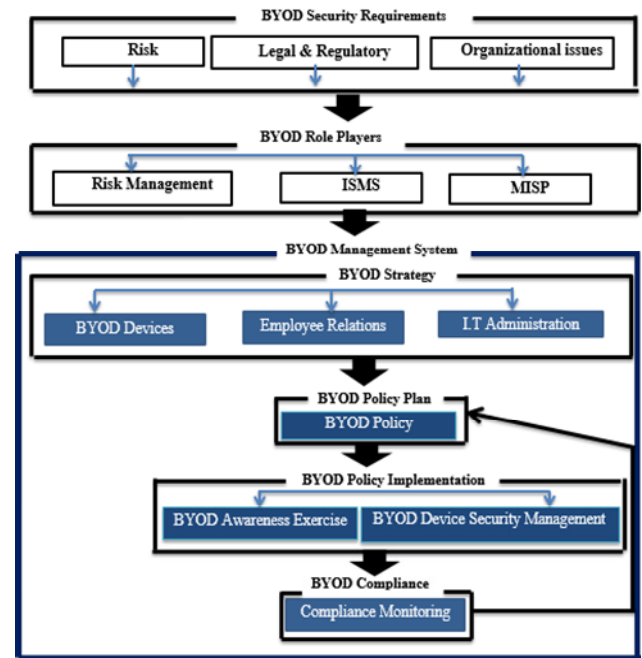


Figure 5: BYOD high level management framework

Figure 5 illustrates the BYOD high level management framework. The BYOD high level management framework is divided into six sections; the BYOD Security Requirements, Security Role Players, BYOD Strategy and the BYOD Policy

Plan, BYOD Policy Implementation and BYOD Compliance. The purpose of the BYOD strategy is for executive management to make all the decisions that are required for the governance of BYOD. The decisions to be made should take into account the following three components; BYOD Devices, Employee Relations and IT Section. The six components will be further divided into the following:

- **BYOD Security Requirements:**
 - **Risk:** Determine risks to the CIA of the information
 - **Legal & Regulatory issues:** Identify legal and regulatory issues
 - **Organizational issues:** Identify other security requirements
- **BYOD Role Players:**
 - **Risk Management:** Identify BYOD risks
 - **ISMS:** Secure organizational information
 - **MISP:** Determine what the MISP states about information security
- **BYOD Strategy:**
 - **BYOD Devices:**
 - **Type of device:** Decisions about the type of device to be incorporated into the municipal environment for BYOD.
 - **Device registration:** It is essential that the preferred devices are registered.
 - **Employee Relations:**
 - **Eligibility and Registration:** Decisions need to consider the eligibility of employees and the registration of the eligible employees.
 - **Awareness Programs:** Executive management must decide on the awareness programs.
 - **IT Section:**
 - **Compatibility testing:** The BYOD devices require compatibility testing.
 - **Authentication and Authorization:** BYOD users need to be authenticated and authorized.
 - **Information separation:** Information should be separated on the BYOD device.
 - **Device and Application Management / Security:** The information and applications within the BYOD device, require constant security and protection.

Once the decisions are concluded, a draft of a BYOD Policy should follow. The BYOD Policy will be inclusive but not limited to the policies, controls, education and control measures. The BYOD Policy can be divided into the following components:

- **BYOD Policy Plan:**
 - **BYOD Policy:** A BYOD Policy should be a documented guideline for BYOD.

- **BYOD Implementation:**

- **BYOD Awareness Exercise:** This component will consist of the educational, awareness and training aspects of BYOD.
- **BYOD Device Management:** BYOD device management will be addressed in this component.

- **BYOD Compliance:**

- **Compliance Monitoring:** There needs to be constant monitoring of compliance for BYOD.

The BYOD high level management framework was formulated under the design-oriented research paradigm. The identified SMME environment and stakeholder for this study is local government, particularly at a District Municipality, situated in the Southern Cape. The District Municipality is applicable to this study because currently there is no BYOD management in place in local government and has aspects that pertain that it as an SMME.

The initial draft of the framework was based on a literature study, which was further justified through a process of cycles of refinement. The literature study and initial draft of the framework was presented during a visit to the District municipality. The literature study portrayed that there are various components that are composed within a BYOD framework. Therefore, a mind map of all the different components was illustrated.

A mind map also known as “brain map” or “mental map” was developed by Tony Buzan during the 1970s. It can be defined as an outline with ideas and pictures radiating out from a central concept (main idea). From the central concept key ideas radiate out, like the branches of a tree. The branches contain key words written in capitals over the line. [29].

Once the mind map has been drafted, a focus group was scheduled to substantiate the components on the mind map. A definition for a focus group is as follows; “*a group of interacting individuals having some common interest or characteristics, brought together by a moderator, who uses the group and its interaction as a way to gain information about a specific or focused issue*” [30]. Following the implementation of the focus group, a survey questionnaire was formulated which was inclusive of the proposed components to be contained in the framework. The questionnaire was constructed on an Excel spreadsheet and divided into the three components: BYOD Policy, BYOD Awareness Exercise and the BYOD Device Management interlaced in the BYOD Policy Plan hierarchy.

A second visit was scheduled to the District Municipality where formal semi-structured interviews were conducted with two representatives from the municipality. The semi-structured interview lasted approximately an hour and data was gathered through a survey questionnaire. The purpose of the semi-structured interviews was to further analyse a suitable solution for the municipal environment. An illustration of the process towards the implementation of the BYOD high level management framework discussed above is represented in Figure 6.

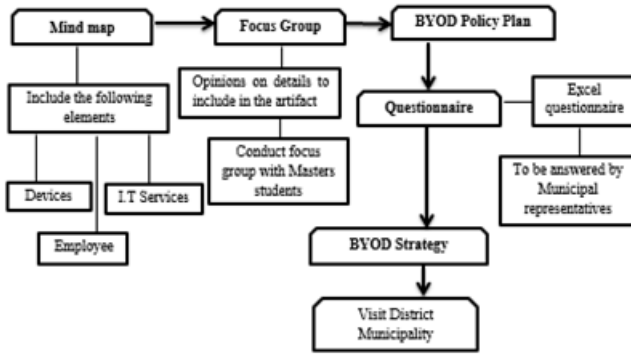


Figure 6: Process model for the BYOD high level management framework

The proposed BYOD high level management framework is a solution that wants to govern and manage BYOD within an SMME related environment. The previous section discussed four frameworks existing in literature that also aim to govern and manage BYOD. The upcoming section will provide an evaluation of the four existing frameworks in literature and the BYOD high level management framework.

IV. EVALUATING FRAMEWORKS FOR BYOD

BYOD is a phenomenon that warrants constant management and governance. The previous section, proposed a BYODMS framework and the preceding section provided four existing frameworks in literature. Consequently, when compared to the four existing frameworks in literature, the development of the BYOD high level management framework raises the question; is it a suitable solution compared to the solutions that currently exist? Therefore, this section will provide a critical evaluation of the BYOD high level management framework against the four existing frameworks discussed earlier in the paper.

Each of the four existing frameworks in literature and the BYOD high level management framework, have their benefits and when compared to each other, there are similarities that can be observed. Furthermore, the observation findings from the four existing frameworks provide elements that can be deemed as missing from the frameworks. Consequently, the BYOD high level management framework has been adapted to bridge the missing elements by fulfilling the eight BYOD characteristics an organization must follow for governing BYOD. Furthermore, when formulating the BYODMS, the SMME context was taken into account. Table 3 tabulates the similarities and missing elements between the BYOD high level management framework and the four existing frameworks from literature.

Table 3: Evaluation of frameworks

Frameworks	Similarities to BYOD high level management framework	Missing elements
BYOD security framework [5]	<ul style="list-style-type: none"> - Understands the business environment. - Registers BYOD devices - The organization has measures for device and information protection - Organizations provides continuous monitoring. 	<ul style="list-style-type: none"> - The framework is technical aspect of governing BYOD devices. - The SMME environment is not cited.
BYOD framework for a management system [24]	<ul style="list-style-type: none"> - Determine threats through a risk assessment - Develop strategies or policies for the governance of BYOD - Planning before policy implementation. An evaluation of the strategy. 	<ul style="list-style-type: none"> - The role of compliance isn't considered. - Adoption in an SMME environment is not cited.
BYOD privacy & culture governance framework [25]	<ul style="list-style-type: none"> - Determine the culture of the organization - Provide a clear definition for the respective privacy concerns - Develop a policy 	<ul style="list-style-type: none"> - The employee role is not considered. - The SMME environment is not cited.
Enterprise and BYOD space BYOD security framework [26]	<ul style="list-style-type: none"> - The organizational context must be considered. - There is a BYOD device analysis and IT administration. - There is a BYOD policy in place. - Compliance is incorporated. 	<ul style="list-style-type: none"> - There is a lack of adequate risk management. - The SMME environment is not cited.

The evaluation of the four existing frameworks in literature against the BYOD high level management framework tabulated in Table 3, indicate that they seemingly lack in addressing BYOD within an SMME environment. It could be hypothesized that the existing frameworks in literature address the governance of BYOD within large organizations. Thus, it can be determined that the BYOD high level management framework is the appropriate solution for the governance of BYOD in SMMEs. Furthermore, the BYOD high level management framework was developed with the eight BYOD characteristics in mind. Therefore, the BYOD high level management framework meets the eight BYOD characteristics that an organization should follow when implementing a governance oriented solution for BYOD in SMMEs.

V. CONCLUSION

BYOD is redefining how employees and organizations conduct daily business tasks. The adoption of BYOD in both large and small organizations governs an era where the filtration of personal and business is becoming blurry. The

risks associated to BYOD are undeniable. But, with proper governance, BYOD can be managed.

This paper studied and discussed the BYOD phenomenon and how BYOD is affecting SMMEs. It was derived that there is a need for a BYOD solution within an SMME environment and the solution should adhere to eight BYOD characteristics. As a result, four existing frameworks in literature were studied to determine if there is a solution that exists and meets the eight BYOD characteristics for an SMME BYOD solution. Once it was concluded that the four existing frameworks meet some of the characteristics but not all, the BYOD high level management framework was formulated. Following the formulation of the BYOD high level management framework, there was an evaluation of the frameworks for BYOD. Thus, it was determined that the BYOD high level management framework is an appropriate solution for BYOD. For future work, a suggestion of the formulation of a BYOD policy for SMMEs.

REFERENCES

- [1] D. Palacios-Marqués, P. Soto-Acosta, and J. M. Merigó, "Analyzing the effects of technological, organizational and competition factors on Web knowledge exchange in SMEs," *Telemat. Informatics*, vol. 32, no. 1, pp. 23–32, 2015.
- [2] L. A. Joia, "Measuring intangible corporate assets, linking business strategy with intellectual capital," *Intellect. Cap.*, vol. 1, pp. 68–84, 2000.
- [3] B. M. B. Suhail Qadir Mir, Mehraj-ud-din Dar, S M K Quadri, "Information availability: Components, Threats and Protection mechanisms," *J. Glob. Res. Comput. Sci.*, vol. 2, no. 3, 2011.
- [4] E. Fakhrutdinova, J. Kolesnikova, O. Yurieva, and A. Kamasheva, "The Commercialization of Intangible Assets in the Information Society," *World Appl. Sci. J.*, vol. 27, pp. 82–86, 2013.
- [5] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "BYOD security engineering: a framework & its analysis," *Comput. Secur.*, vol. 55, pp. 81–99, 2015.
- [6] K. Madzima, M. Moyo, and H. Abdullah, "Is Bring Your Own Device an institutional information security risk for small-scale business organisations?," 2014.
- [7] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments," *J. Inf. Priv. Secur.*, vol. 11, no. 1, pp. 38–54, 2015.
- [8] *The Role of IS Assurance & Security Management*, vol. 1, 2013.
- [9] A. A. Dedeché, F. Liu, M. Le, and S. Lajami, "Emergent BYOD Security Challenges and Mitigation Strategy Research Methodology," pp. 1–17, 2013.
- [10] B. Van Ommen, "IT Security in SMEs: Necessary or Irrelevant?," 2014.
- [11] *National Small Business Amendment Act*, 2004.
- [12] J. Devos, H. Van Landeghem, D. Deschoolmeester, and J. Devos, "Rethinking IT governance for SMEs," *Emerald*, 2012.
- [13] S. Kabanda and I. Brown, "Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries – The Case of Tanzania," in *25th Australasian Conference on Information Systems*, 2014.
- [14] T. A. Yang, R. Vlas, A. Yang, and C. Vlas, "Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior," *Proc. - Soc.* 2013, pp. 411–416, 2013.
- [15] S. Allam, S. V. Flowerday, and E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," *Comput. Secur.*, vol. 42, pp. 55–65, 2014.
- [16] M. Hensema, "Acceptance of BYOD among Employees at Small to Medium-sized Organizations," *19th Twente Student Conf. IT*, pp. 1 – 8, 2013.
- [17] M. A. Harris, K. Patten, and E. Regan, "The Need for BYOD Mobile Device Security Awareness and Training," in *Proceedings of the Nineteenth Americas Conference on Information Systems*, 2013, no. January.
- [18] A. Weeger and H. Gewald, "Factors Influencing Future Employees Decision-Making to Participate in a BYOD Program: Does Risk Matter?," 2014, pp. 0–14.
- [19] S. Charbonneau, "The role of user-driven security in data loss prevention," *Comput. Fraud Secur.*, vol. 2011, no. 11, pp. 5–8, 2011.
- [20] Eslahi Meisam, Var Naseri Maryam, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current State and Security Challenges," *IEEE Symp. Comput. Appl. Ind. Electron.*, pp. 189–192, 2014.
- [21] K. Dulaney and P. Debeasi, "Managing Employee-Owned Technology in the Enterprise," 2011.
- [22] A. C. Johnston, M. Warkentin, and M. Siponen, "AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK : LEVERAGING THREATS TO THE HUMAN A SSET THROUGH SANCTIONING RHETORIC," vol. 39, no. 1, pp. 113–134, 2015.
- [23] A. M. French, C. Guo, and J. P. Shim, "Current Status , Issues , and Future of Bring Your Own Device (BYOD)," *Commun. Assoc. Inf. Syst.*, vol. 35, 2014.
- [24] M. Brodin, "Combining ISMS with strategic management : the case of BYOD COMBINING ISMS WITH STRATEGIC MANAGEMENT : THE CASE OF BYOD," no. August, 2015.
- [25] N. Selviandro, G. Wisudiawan, S. Puspitasari, and M. Adrian, "Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control," in *2015 3rd International Conference on Information and Communication Technology (IColCT)*, 2015, pp. 113–118.
- [26] Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," *2014 IEEE 11th Consum. Commun. Netw. Conf.*, pp. 80–85, 2014.
- [27] M. Brodin, "Management issues for Bring Your Own Device," 2015.
- [28] H. Österle, J. Becker, U. Frank, T. Hess, D. Karagiannis, H. Kremer, P. Loos, P. Mertens, A. Oberweis, and E. J. Sinz, "Memorandum on design-oriented information systems research," *Eur. J. Inf. Syst.*, vol. 20, no. 1, pp. 7–10, 2011.
- [29] M. Davies, "Concept mapping, mind mapping and argument mapping: What are the differences and do they matter?," *High. Educ.*, vol. 62, pp. 279–301, 2011.
- [30] M. a Masadeh, "Focus Group : Reviews and Practices," *Int. J. Appl. Sci. Technol.*, vol. 2, no. 10, pp. 63–68, 2012.