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].

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

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:

<u>BYOD Characteristics:</u>

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 increases 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].

978-1-5090-2473-8/16/$31.00 ©2016 IEEE

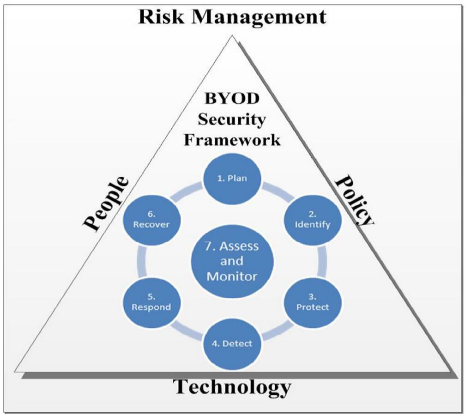

Figure 1: BYOD Security Framework [5]

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.

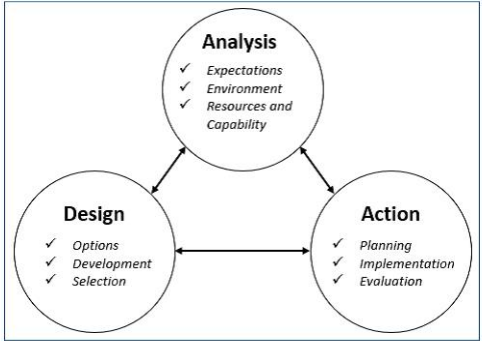

Figure 2: BYOD framework for a management system [24]

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.

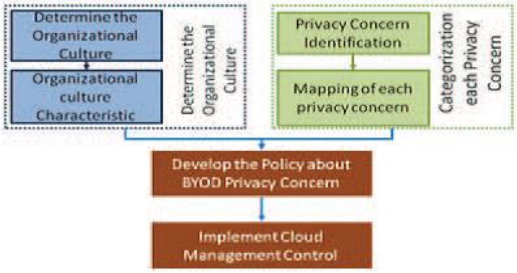
Determine the Organizational Culture
Organizational culture Characteristic
Determine the Organizational Culture
Privacy Concern Identification
Mapping of each privacy concern
Categorization each Privacy Concern
Develop the Policy about BYOD Privacy Concern
Implement Cloud Management Control

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].

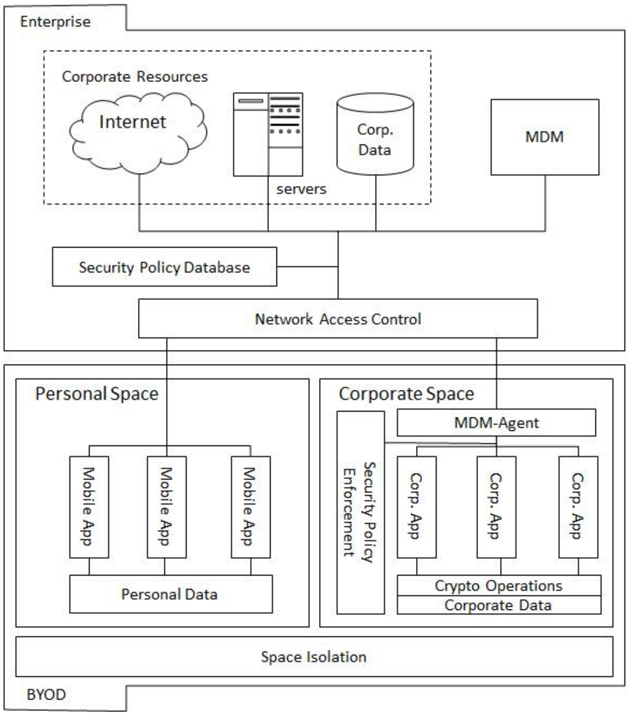

Figure 4: Enterprise and BYOD space BYOD Security Framework [26]

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 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].

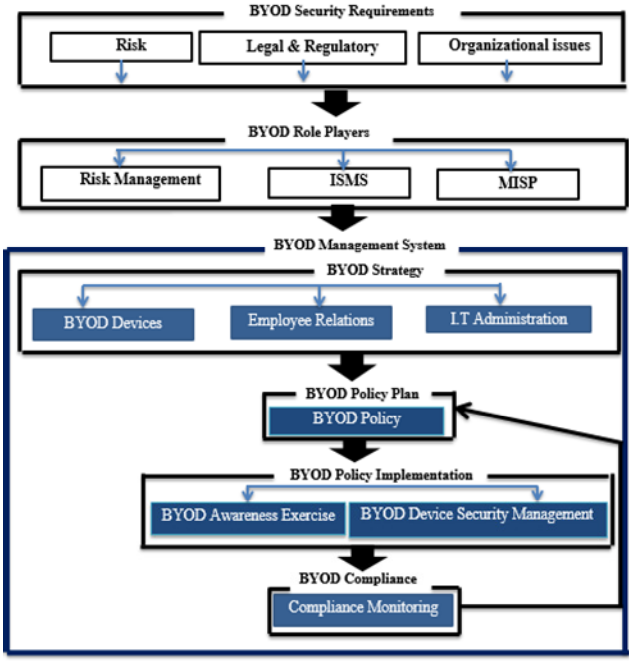

Figure 5: BYOD high level management framework

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: I**nformation 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.

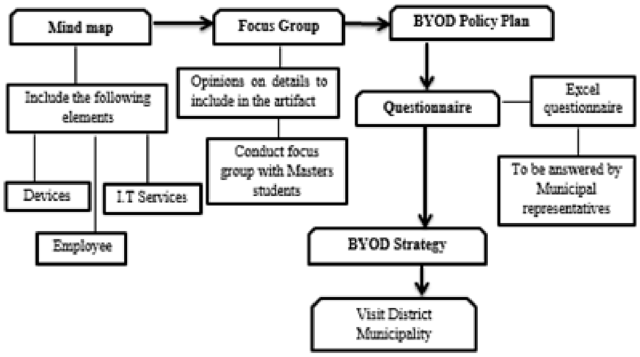
Mind map
Focus Group
BYOD Policy Plan
Include the following elements
Opinions on details to include in the artifact
Questionnaire
Excel questionnaire
Conduct focus group with Masters students
Devices
I.T Services
Employee
To be answered by Municipal representatives
BYOD Strategy
Visit District Municipality

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 in 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]	- Understands the business environment. - Registers BYOD devices - The organization has measures for device and information protection - Organizations provides continuous monitoring.	- The framework is technical aspect of governing BYOD devices. - The SMME environment is not cited.
BYOD framework for a management system [24]	- Determine threats through a risk assessment - Develop strategies or policies for the governance of BYOD - Planning before policy implementation. An evaluation of the strategy.	- The role of compliance isn't considered. - Adoption in an SMME environment is not cited.
BYOD privacy & culture governance framework [25]	- Determine the culture of the organization - Provide a clear definition for the respective privacy concerns - Develop a policy	- The employee role is not considered. - The SMME environment is not cited.
Enterprise and BYOD space BYOD security framework [26]	- 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.	- 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. Dedeche, 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 (ICoICT)*, 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. Krcmar, 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.