Review of Data Storage Protection Approaches for POPI Compliance

Nicholas Scharnick
Centre for Research in Information and Cyber Security
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s209012789@nmmu.ac.za

Mariana Gerber
Centre for Research in Information and Cyber Security
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Mariana.Gerber@nmmu.ac.za

Lynn Futcher
Centre for Research in Information and Cyber Security
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Lynn.Futcher@nmmu.ac.za

Abstract—**In business, information security has always been a debated topic amongst management and executives. Investing in something that is intangible is often not seen as priority expenditure as it brings no Return on Investment nor contributes to expanding the business. However, the newly enacted Protection of Personal Information (POPI) Act forces businesses to re-evaluate their stance on information security and data storage protection as POPI requires that "appropriate and reasonable security measures" be put in place to effectively protect all personal information that large organisations as well as smaller businesses process and more importantly store. However, the lack of comprehensive controls found within any one information security approach (information security standard, best practice or framework) to fully address the requirements of the POPI act, leaves businesses exposed to legislative action under POPI.**

This paper, through the use of a detailed literature review and qualitative content analysis aims to analyze widely implemented information security approaches in the context of POPI compliance. Through identifying themes for data protection within various information security approaches, an evaluation of the comprehensiveness of these approaches and their proposed mechanisms for protecting data within businesses is conducted.

Keywords: Legislation; POPI; Information Security; Business; Data; Data Security; Storage Protection.

I. INTRODUCTION

Businesses are an important aspect of an economy in any country, without them minimal economic growth can occur. In South Africa, the largest business contributors are Small, Medium and Micro Enterprises (SMMEs), as these types of businesses make up 91% [1] of all business entities in South Africa, emphasizing the importance of assisting and supporting all business sizes in order to keep growing the economy.

In today's competitive business landscape, technology can prove to be a major asset in conducting and growing an established or newly started business. Technologies such as Information Technology (IT) and IT systems have always had a place in any business; however, traditionally placed as a mechanism to support the business operations. With the rapid evolution of modern technology, businesses now consider IT as an invaluable resource [2], thus IT has moved from a supporting role to a key driving force within the business [3], reaching a point where businesses rely on IT to conduct business. This newly found reliance on IT brings with it a fair number of concerns, including IT security, mismanagement of these systems as well as data protection [4], [5], [6].

This paper investigates how the issues of data storage and data protection within businesses, specifically SMMEs, can be addressed using various information security standards, best practices and frameworks in light of the recently enacted Protection of Personal Information (POPI) Act.

II. RESEARCH METHODOLOGY

For the purpose of this study, a background literature review was conducted in order to gain an understanding of the fundamental principles of information security and data protection. A further literature study was conducted on the recently enacted POPI Act in order to determine the current perception of the Act as well as what the act requires of a business in order to achieve compliance when protecting stored data. Upon determining the requirements for POPI compliance, specifically for protecting stored data, literature was consulted in order to determine which information security standards, best practices and frameworks are being widely adopted by businesses across the globe. Through the identification of such security approaches, the content thereof was analyzed using a qualitative content analysis. A qualitative content analysis can be defined as "A research technique for making replicable and valid inferences from texts to the contexts of their use" [7]. This analysis aimed to identify specific themes which relate to data, data security, protection of data and protecting Personally Identifiable Information (PII) found within the determined security approaches. The identified themes were then summarized within each analyzed information security approach along with the section in which they are located in the respective information security approach. Finally, all information security approaches and the themes identified are summarized to provide a holistic view of the comprehensiveness of addressing data protection.

III. BACKGROUND

The importance of IT in today's modern businesses coupled with the interconnectedness of society and the rapid expansion of the internet and internet based services, social media and networking leads businesses toward adopting IT based solutions in order to remain competitive in an e-commerce driven society. In business, an IT solution can provide a range of benefits, these include cultivating cost effective solutions to the businesses processes, reducing the overhead of business activities through efficient business practices and streamlining business processes through the incorporation of an IT solution [8]. However, should an IT solution be considered, the business needs to keep in mind that these advantages can be overshadowed by potential areas of concern that come with an IT solution. An organisation needs to consider the security implications of implementing an IT solution and ensure these security related concerns are addressed. Not only do these concerns need to be addressed, the organisation should consider the implementation of good information security practices in order to maintain the security of any information assets within the business as well as ensuring proper management of such security implementations.

Information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" [9]. Further, the three traditional characteristics at the core of information security, namely Confidentiality, Integrity and Availability (CIA) also need to be upheld and preserved [10]. In order for a business to address any information security concerns that arise from implementing an IT solution, the information security requirements of the business need to be established. Information security requirements are seen as "The amount of security needed to provide the required level of information security" [11]. To determine the appropriate "amount" of security that the business needs, the three originating sources that comprise information security requirements need to be considered. These three sources are stated as [10]:

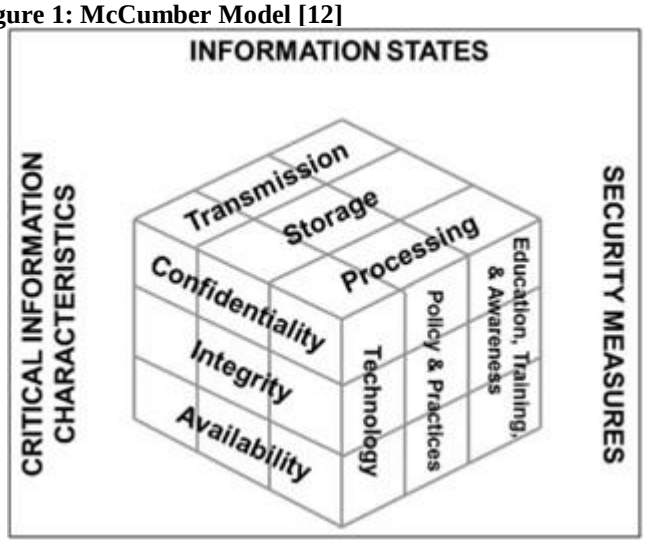
- Assessing risks to the business, while considering the business goals and objectives.
- Legal, regulatory and contractual requirements that the business has to satisfy.
- Principles, objectives and business requirements that support the business's operations.

The definition of information security and information security requirements highlights that security is an ever important aspect that has to be considered in the modern and fully digital era that we live in. Thus the protection of a business's information assets becomes a key factor that needs to be addressed when considering how critical these information assets are in modern day business.

When considering "data" and "information" these terms are sometimes used interchangeably. However, these terms bring separate meanings within the context of an information asset. Information assets need to be protected as they originate from data which is then processed into a meaningful context. However, not all types of data require some form of processing (producing information from data) in order to become an information asset. These types of data include: PII such as names, addresses and identification numbers, credit card details and banking details. These types of data are not contextualized through processing (thus becoming information) yet still hold value to a business, thus becoming an asset.

These information assets can be in a variety of forms within a business as there are three primary "states" that digital information can be in at any time. These states are: storage transmission and processing and are also known as data at rest, in motion and in use. The McCumber model [12], illustrated in Figure 1, depicts the three states of information in the context of the characteristics of information security as well as information security measures to maintain good information security practices within the business.

Figure 1: McCumber Model [12]



Focusing on the state of "Storage", the business needs to consider upholding the three core characteristics of information security through the implementation of good information security practices. Such practices can be a combination of technological information security measures, sound information security policies and ensuring all employees are trained and educated on good information security practices and are aware of any information security concerns. During the process of determining the business security requirements for stored information, the business needs to address any legal requirements that are identified. Should the business store any PII, it needs to address its legislative requirements by complying to the recently enacted POPI Act [1.].

IV. PROTECTION OF PERSONAL INFORMATION

In order for the business to remain competitive and leverage all resources available, IT needs to be adopted [2]. As mentioned, IT provides a wide variety of advantages to the business, thus making the adoption and implementation of these systems more compelling to managers and business owners alike. However, the business has to consider the implications of implementing IT, addressing any concerns that there might be as well as ensuring that any compliance

requirements are met. This highlights a new challenge for businesses, addressing the legislative compliance requirements set out by the POPI Act. The POPI Act was signed into effect on 27 November 2013 and provides legislation on the protection of personal information in South Africa. While the Act has not yet been fully implemented or compliance enforced due to the act requiring the establishment of an information regulator, a large majority of the Act has not yet commenced. This will only occur once the regulator has been put in place and an official commencement date has been announced by the South African President. However, certain sections of the Act such as those pertaining to the establishment of the information regulator have commenced.

Currently, there are a limited number of sections within the POPI Act that have commenced, these being the following:

- Chapter 1: Definitions
- Chapter 5: Supervision: Part A – Information Regulator
- Chapter 12: General Provisions: Section 112 - Regulations
- Chapter 12: General Provisions: Section 113 – Procedure for making regulations
- Chapter 12: General Provisions: Section 113 – Procedure for making regulations

Within the POPI Act, there are two major sections that deal with the security aspect of information. The first is Chapter 3, titled "Conditions for lawful processing of personal information" which is divided into three parts. Part A contains several "conditions" numbered 1 to 8 as subsections and focuses on processing personal information from a general perspective. Part's B and C focus on processing of special personal information and personal information of children respectively. The second being Chapter 9: "Trans-border informational flows" which outlines the requirements of a business should personal information be transferred to a third party residing in a foreign country.

Approaching Chapter 3 of the Act from the perspective of information security, an important "condition" within Part A of the Act, being Condition 7: "Security safeguards" is of significance. This condition provides legislative guidance and security requirements for businesses when processing or storing personal information. The condition has 4 subsections that relate to security. When considering data storage, Subsection 19 of the condition addresses security measures that pertain to maintaining the integrity as well as confidentiality of any personal information within an organisation. The requirements outlined by Subsection 19 ensure that confidentiality and integrity of information is maintained while at the same time the business takes "appropriate, reasonable, technical and organizational measures" [13] to prevent loss, damage, unauthorized destruction and unlawful access to any personal information held by the business.

Looking at the above statement taken from the Act, what is required for compliance is unclear and can be interpreted in many ways. The Act does not define what is seen as "appropriate, reasonable, technical and organizational measures" and could lead to uncertainty and confusion for business owners and managers alike. In business this can easily occur as having insufficient knowledge or expertise on the security domain can hinder the understanding of what is required in order to implement "appropriate, reasonable, technical and organizational" measures for protecting personal information within the business.

Subsection 19 does provide limited guidance on addressing such concerns, stating that all foreseeable risks to the information held by the business are identified and that appropriate safeguards are put in place to mitigate such risk to the personal information. Further, the Act states that the business should ensure that such safeguards are effective in preventing or mitigating the associated risk and ensure that they are continually updated for such purpose.

Finally, the Act states that an organisation "must have due regard to generally accepted information security practices and procedures" [13] and ensure that any industry or profession related requirements are complied with when regarding good security practices.

Achieving compliance to POPI can be a demanding task as once again, there is a definitive lack of detail within the "guidance" for businesses to follow in order to become compliant with the requirements of the POPI Act. Considering that all businesses are required to comply with what is set out in the POPI Act, coupled with the legislative action that could be taken against businesses for non-compliance; places more strain on these businesses.

V. Approaches for POPI Compliance

Addressing the legislative compliance requirements of POPI can be done using one of the many well established information security approaches found within the information security domain. Some of the better recognized and more mature approaches will be analyzed and discussed in detail, placing focus on various themes found within these approaches that aim to address information security from a data protection perspective. The approaches discussed include key role players namely ISO, NIST, COBIT and ITIL.

A. ISO 27000 series of standards

The International Organisation for Standardization (ISO) 27000 standards are a series of best practice standards aimed at providing recommendations for the management of various information security topics within businesses [14]. Notable standards within the 27000 series are ISO27001, ISO27002 and ISO 27040. These standards address the implementation of an Information Security Management System (ISO 27001) [15], providing a code of practice for information security within a business (ISO 27002) [10] and providing guidance for storage security within the business (ISO 27040) [16].

Within these three ISO standards, a variety of data protection related themes can be found. Such themes provide guidance to the business on better protecting any business related data.

TABLE I. ISO 27000 SERIES THEMES

Themes	Source
Access Control	27002
Awareness and Training	27001/27002
Backup	27002
Data Confidentiality and Integrity	27040
Data Reliability and Availability	27040
Data Retention	27040
Information Protection	27002/27040
Media Handling	27002
PII	27002
Storage Management	27040

Referring to Table I, the themes drawn from the ISO 27000 series addresses the three main aims of information security, those being to ensure the confidentiality, integrity and availability of information. From the legislative aspect and specifically POPI, ISO provides guidance on PII. Considering the themes found in Table I, the ISO 27000 series addresses data protection from various angles, ensuring access control measures are in place, providing for retention and backup procedures as well as ensuring the business is aware of security concerns and trained to practice sound information security.

B. NIST

The National Institute of Standards and Technology (NIST) is a United States institution that aims to develop documentation and guidance on various security concerns. While there are a range of publications by NIST that address a wide variety of security related topic areas, Special Publication (SP) 800-122 and 800-171 focus on PII. PII is defined as "any information about an individual maintained by an organisation, which includes any information that can be used to distinguish or trace an individual's identity" [17].

TABLE II. NIST THEMES

Themes	Source
Access Control	SP800-171
Awareness and Training	SP800-171/122
Breach Protection	SP800-122
Identification and Authentication	SP800-171
Information Confidentiality	SP800-122
Information Integrity	SP00-171
Media Protection	SP800-171
Personnel Security	SP800-171
PII Protection	SP800-122/171
Physical Protection	SP800-171
Privacy	SP800-122

Similar to the themes identified within the ISO series of standards, the NIST publications address aspects that are core to good information security practices. Protecting the confidentiality and integrity of any information within the business is of the utmost importance. Table II highlights an array of themes identified within the NIST publications which provide guidance for protecting data in the business. Key themes to note are breach protection and physical protection, ensuring physical hardware is secure and protected as well as virtual access is secured with the appropriate technical measures such as firewalls, encryption and other mechanisms.

C. COBIT

The Control Objectives for Information and Related Technology framework, or better known as COBIT, is a framework developed in 1996 by the Information Systems Audit and Control Association (ISACA). COBIT aims to provide a comprehensive and holistic approach to governing and maintaining IT within the organisation [18]. The most recent iteration of the framework, COBIT 5 contains five main principles. These principles include:

- Meeting stakeholder needs;
- Covering the enterprise end-to-end;
- Applying a single integrated framework;
- Enabling a holistic approach;
- Separating governance from management.

The COBIT framework contains control objectives for various topic areas and scenarios within the business. The major domains that these control objectives cover include: planning and organisation, acquisition and implementation, delivery and support; and monitoring.

TABLE III. COBIT THEMES

Themes	Source
Access Control	DS 11.6
Backup	DS 11.25
Data Integrity	DS 11.30
Storage Management	DS 11.19

The five main principles of COBIT suggest that the framework is more business oriented, focusing on aspects of the business such as ensuring full coverage of the enterprise as well as addressing its stakeholder's needs. However, the COBIT framework does provide some guidance on information security within the business, including some basic aspects of data protection.

Table III summarizes the identified themes within COBIT, which include ensuring that the integrity of data is upheld, managing storage and backup of data as well as implementing access control measures within the organisation.

D. ITIL

The Information Technology Integrated Library (ITIL) is an IT service management framework that is widely adopted worldwide and aims to provide businesses with a practical approach to the identification, planning, delivery and support of IT services within businesses [19]. The ITIL framework is comprised of five volumes, covering major IT related areas such as: service design, strategy, operation and transition, as well as providing continual service improvement. When considering the ITIL framework from an information security perspective, each of the five volumes contributes to this topic in some form. However, service design and specifically Section 4.6 of this volume contributes to this in a major way. This includes guidance for an Information Security Management System (ISMS) within the organisation as well as an information security policy [20].

TABLE IV. ITIL THEMES

Themes	Source
Access Control	Section 4.5
Breach Protection	Section 4.6.5.2
Policy/Procedures/Controls	Section 4.6.4/4.6.5.1

The ITIL framework focuses on the topic of IT in the business, with the aim of ensuring the IT systems and services function effectively and are managed in such a way that supports this aim. Considering the identified themes; Table IV highlights that within ITIL there is little focus on information security, taking a similar approach as with COBIT by providing the basic guidance on security measures within the organisation. Thus ensuring appropriate access control and breach protection measures are put in place through the effective use of policies and controls.

VI. SUMMARY

Table V summarizes the themes found within each of the four reviewed information security approaches, providing a complete picture on the extent of guidance provided for data protection within each approach.

As previously mentioned, ISO and NIST have published a wider variety of documents for a range of security topics. Thus as seen in Table V, the approaches provided by these two bodies are more comprehensive in addressing security concerns specific to data protection over their counterparts COBIT and ITIL. However, this does not make any one standard, a superior choice over any other as an important point to note is “Every business has distinct data protection, backup and recovery needs and there is no one-size-fits-all solution” [21].

Table V provides an overview of the themes found within each of the four information security approaches. However, each information security approach addresses the identified themes in different ways. To follow, a comparative summary describes how each security approach addresses a specific theme in relation to each of the other approaches.

A. Access Control

The ISO series of standards addresses access control mechanisms for data protection within ISO27002. Providing generalized guidance on implementing controls for restricting access to information through the controlling of access rights of users as well as other applications. The NIST publication SP800-171 details access control requirements for protecting controlled unclassified information and takes a more detailed and technical approach over its ISO27002 counterpart.

TABLE V. SUMMARY OF THEMES

Thenes	ISO	NIST	COBIT	ITIL
Access Control	27002	SP800-171	11.6	4.5
Awareness and Training	27001/27002	SP800-122/171		
Backup	27002		11.25	
Breach Protection		SP800-122		4.6.5.2
Data Confidentiality and Integrity	27040	SP800-122/171	11.30	
Data Reliability and Availability	27040			
Data Retention	27040			
Identification and Authentication		SP800-171		
Information Protection	27002/27040			
Media Handling	27002	SP800-171		
Personnel Security		SP800-171		
Physical Protection		SP800-171		
PII	27002	SP800-122/171		
Privacy		SP800-122		
Storage Management	27040		11.19	

SP800-171 states 22 requirements when addressing access control, these include:

- Monitor and control remote access sessions;
- Limit unsuccessful logon attempts;
- Encrypt controlled unclassified information on mobile devices.

However, COBIT and ITIL both address access control from a broader more business orientated perspective. The COBIT framework provides some basic requirements for a business to follow for addressing access control. While the approach of ITIL extends the businesses information security policies through access management, the ITIL approach does not set policies for access control but merely executes the information security policies already defined within the business.

B. Awareness and Training

The theme of awareness and training are covered fairly broadly within ISO and NIST. ISO27001 and ISO27002 both provide guidance for training and awareness within the business. ISO27001 focuses on this from the perspective of the Information Security Management System (ISMS), stating that all employees with responsibilities defined within the ISMS are competent to perform such duties.

ISO27002 approaches awareness and training by first ensuring employees are aware of the businesses security policies and procedures before being granted any access to information. ISO27002 also states that ongoing training should occur, ensuring employees are aware of any business related controls in place as well as its legal responsibilities. This especially holds true for the POPI Act, as it is the businesses legal responsibility under the POPI Act to protect any personal information stored within the business.

NIST SP800-122 states that "Awareness, training, and education are distinct activities, each critical to the success of privacy and security programs" [17]. From the viewpoint of POPI, it is imperative that the businesses employees are sufficiently trained to carry out and adhere to their responsibilities to protect any personally identifiable information or risk legislative action.

C. Backup

ISO27002 and specifically Section 10.5 of the standard, aims to address the topic of backup, providing guidance to the organisation with the objective of maintaining the integrity and availability of the information. In order to accomplish this, the guidelines put forward ensure that the frequency of performing backup's falls in line with the business requirements. These guidelines also emphasise the importance of implementing an appropriate amount of physical and virtual security, while ensuring that the reliability of any backed up data is regularly tested.

Within the COBIT control objectives, DS11.25 addresses "Back-up Storage", highlighting that back-up procedures should include the proper storage of data files and any related documentation. Further, DS11.25 states that the storage sites for any backup data should be periodically reviewed to ensure the effectiveness of all security measures.

D. Breach Protection

Breach protection from the context of data protection is not addressed comprehensively within any of the four security approaches that were analyzed. ITIL makes mention of the management of security breaches within Section 4.6.5.2. Similarly, NIST approaches breach protection from a management perspective, stating that management of such breaches would require "coordination among personnel from across the organization" to ensure effective management of such an incident. However, NIST does state that breaches which involve PII need to be handled in an alternative manner. This is due to the potential sensitivity of the information as well as the possible impact such an incident might have on the business. From the perspective of POPI, should such a breach occur, notification to the information regulator as well as the data subject(s) involved needs to be made in accordance to Section 22 of the Act.

E. Data Confidentiality and Integrity

Within the NIST Special Publication 800-122, a section entitled "PII Confidentiality Safeguards" discusses two major options that organisations can select from in order to address PII concerns and maintain the confidentiality of any PII that it holds. The first option available to organisations is to develop various policies and procedures to address the concerns they have regarding the PII within the business. This would then serve as the "rules" to follow in order to protect the confidentiality of any PII.

The second approach that organisations can opt for is education, awareness and training programs for their employees. Such programs should focus on methods to ensure confidentiality as well as making employees aware of any potential security threats that could impact the confidentiality of the PII within the organisation.

COBIT once again takes a business and management approach to providing guidance, stating that the integrity of data be checked periodically.

F. Media Handling

ISO27002 addresses important aspects of media handling which includes the management of any removable media within the business as well as the disposal thereof when it is no longer needed. Guidance provided by the standard for managing any removable media within the business includes ensuring that accurate records are kept for auditing purposes when media is removed from the business by authorized personnel. Media management also includes the security of the physical storage media, storing it in an appropriate manner while keeping it safe and secure.

The NIST Special Publication SP800-171 provides more detailed guidance to the business for protecting its storage media. Stating various technical measures for securing such media while ensuring only authorized personnel have access as well as ensuring that the confidentiality of the information is upheld.

G. Personally Identifiable Information

The ISO27002 standard provides guidance for the development of an organizational privacy policy. This policy can be seen as an important step towards securing the data and more importantly, PII stored within the business. However, a privacy policy needs to be communicated to all employees within the organisation that handle any private information to ensure the effectiveness of the policy and to better protect sensitive personal information. While an organisational privacy policy is important, compliance with all relevant data protection legislation and regulation is crucial.

PII from the NIST perspective "should be protected through a combination of measures". NIST provides guidance for the implementation of operational safeguards as well as detail on policy and procedure creation for protecting PII within the business.

H. Storage Management

Considering the importance of storage in today's modern society, COBIT provides minimal guidance to businesses for addressing this topic. COBIT states that procedures should be developed to address any data storage concerns and ensure effective management thereof.

The ISO 27040 standard provides supporting controls for storage management and aims to address the security requirements of the organisation from a data protection and security standpoint. Once management and administrators are aware of the risks associated with storing information within the business, ISO 27040 strives to provide security guidance for protecting this information.

The summary of these themes provides an overview of each theme as addressed by its corresponding sources, as well as how each source approaches said theme. In order to provide an understanding and detail as to how each of the four security approaches address the topic of data protection, themes that were identified within more than a single security approach were discussed and compared in order to reveal the differences in the guidance provided.

VII. Conclusion

Within this paper, various information security standards, best practices and frameworks were discussed. These best practices aimed at providing guidance to businesses for implementing and maintaining sound information security controls and procedures within the business. This includes guidance on developing and implementing an Information Security Management System as well as implementing various information security controls and procedures to manage and reduce the information security risk of the organisation.

The ISO series of standards also includes ISO 27040. While being a fairly new standard, ISO 27040 sets out to guide businesses in better protecting their stored data by building on and extending the controls found in ISO 27001/2. The topic of protecting data and PII within businesses is of the utmost importance in today's modern and technology centric era. This highlights the need for specific guidance on the topic of data protection. Other major and popular security best practice frameworks were discussed, including the COBIT governance and control framework as well as the ITIL IT service management best practice framework.

Looking at the summarized findings (Table V) one can see that there is "no one size fits all" solution to addressing the protection of data and more specifically, when data is in storage. Should a business organisation want to comprehensively protect any stored data, a combination of the security approaches which have been analyzed within this paper can be applied to address a large majority of the potential areas for security concern.

VIII. Future Research

Future research will focus on data storage and protection within SMMEs in South Africa. Making use of a survey aimed at identifying the types and scales of IT infrastructure within SMMEs and how they address the topics of information security and data protection within the business. The survey will also assist in determining the current understanding of the POPI Act as well as which security approaches SMMEs currently implement with respect to data storage an protection. From the results of the survey, coupled with the themes identified within this research paper, guidelines for SMMEs will be developed which will assist these businesses to better protect any stored data within the organisation, while at the same time also assisting in positioning themselves for the POPI Act and compliance thereto.

IX. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

[1] Abor, J., & Quartey, P. (2010). Issues in SME development in Ghana and South Africa

[2] Nieto, M. J., & Fernández, Z. (2005). The role of information technology in corporate strategy of small and medium enterprises. Journal of International Entrepreneurship, 3(4), 251-262.

[3] Lester, D. L., & Tran, T. T. (2008). Information technology capabilities: Suggestions for SME growth. Institute of Behavioral and Applied Management, 72-88.

[4] Lucchetti, R., & Sterlacchini, A. (2004). The adoption of ICT among SMEs: evidence from an Italian survey. Small Business Economics, 23(2), 151-168.

[5] Hashim, J. (2007). Information communication technology (ICT) adoption among SME owners in Malaysia. International Journal of Business and Information, 2(2), 22

[6] Blackburn, R., & Athayde, R. (2000). Making the connection: the effectiveness of Internet training in small businesses. Education+ Training, 42(4/5), 289-299.

[7] Krippendorff, K. (2012). Content analysis: An introduction to its methodology. Sage.

[8] Bruque, S., & Moyano, J. (2007). Organisational determinants of information technology adoption and implementation in SMEs: The case of family and cooperative firms. Technovation, 27(5), 241-253.

[9] Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

[10] ISO/IEC (2005). ISO 27002: 2005. Information Technology-Security Techniques-Code of Practice for Information Security Management. ISO.

[11] Gerber, M., von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. Information Management & Computer Security, 9(1), 32-37.

[12] NSTISSI No. 4011 (20 June 1994) National training standard for information systems security (InfoSec) Professionals

[13] POPI (2013) "Protection of Personal Information Act", South African Government Gazette (2013) Retrieved from http://www.justice.gov.za/legislation/acts/2013-004.pdf Date retrieved: 12 August 2015

[14] ISO/IEC (2014) ISO 27000: 2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[15] ISO/IEC (2005). ISO 27001: 2005. Information technology — Security techniques — Information security management systems — Requirements

[16] ISO/IEC (2015). ISO 27040: 2015. Information technology -- Security techniques -- Storage security

[17] McCallister, E., Grance, T., & Scarfone, K. A. (2010). SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), National Institute of Standards & Technology, Gaithersburg, MD.

[18] COBIT 5 A Business Framework for the Governance and Management of Enterprise IT (2013).

[19] Arraj, V (2013). ITIL: The basics

[20] Clinch, J. (2009). ITIL V3 and Information Security. Best Management Practice.

[21] "Why SMEs should back up their data to the cloud" (2013, March 11) Retrieved from http://www.theguardian.com/small-business-network/2013/mar/11/back-data-to-cloud-small-business. Date retrieved: 22 March 2015.