A Framework for Information Security Management in Local Government

by

Joshua de Lange

A Framework for Information Security Management in Local Government

by

Joshua de Lange

Dissertation

submitted in fulfilment
of the requirements
for the degree

Master 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

April 2017

Declaration

I, Joshua de Lange, 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.

Joshua de Lange

Abstract

Information has become so pervasive within enterprises and everyday life, that it is almost indispensable. This is clear as information has become core to the business operations of any enterprise. Information and communication technology (ICT) systems are heavily relied upon to store, process and transmit this valuable commodity. Due to its immense value, information and related ICT resources have to be adequately protected. This protection of information is commonly referred to as information security.

Information security risks are a strategic issue which should be thoroughly addressed by all enterprises, public and private in nature. Local government in South Africa are no different. However, the Auditor-General of South Africa deems the majority of information security practices within local government to be inadequate.

Therefore, the objective of this research study was to address this issue by designing an artefact. Consequently, this research naturally followed a design-oriented approach. The artefact of this research took the form of a framework. The framework is titled 'A Framework for Information Security Management in Local Government (FISM)'. FISM was developed in a four-phased iterative approach, in collaboration with stakeholders within local government.

FISM incorporated several criteria which address the unique challenges of local government. These criteria was evaluated by conducting a workshop exercise which was attended by several local government representatives. The results of the validation workshop was good and deemed FISM to adhere to the criteria it set out to meet. Consequently, this research study attained the primary objective it set out to meet, which was to develop FISM in order to address the real-world problem at hand.

Acknowledgements

First and foremost, I want to extend my sincere gratitude to my two supervisors, Prof. Rossouw Von Solms and Prof. Mariana Gerber. Without your continued patience and support,this would not have been possible. I appreciate your insight and guidance throughout this 2 year journey. It was a pleasure to have had the privilege of working under your combined tutelage.

Secondly, I would like to thank the following benefactors for their financial assistance:

- 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.
- The financial assistance of the Nelson Mandela Metropolitan University's Post Graduate Research Scholarship (PGRS) is also hereby acknowledged.
- The financial assistance of Dormehl Cunningham 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 Dormehl Cunningham.

Finally, I want to thank my family for their continued support and faith in me. In spite of all the frustration I caused with all of you, I managed to keep going and was able to see this through because you never doubted me. Your continuous encouragement throughout my years of study is sincerely appreciated. Thank you.

Contents

Declaration **i**

Abstract **ii**

Acknowledgements **iii**

1 Introduction **1**

1.1 Information Security Management and Local Government . . . 1

1.1.1 Layout of Local Government within South Africa . . . 2

1.1.2 Role of ICT in Municipalities 3

1.1.3 Importance of Information Security Management within Local Government 4

1.2 Current Challenges of Local Government 6

1.3 Thesis Statement 6

1.4 Research Objectives 7

1.5 Scope and Delineation 7

1.6 Research Approach 8

1.7 Layout of Dissertation 8

1.8 Conclusion 9

2 Contemporary Information Security Management **11**

2.1 Introduction 11

2.2 The Security of Information and Related Resources 12

2.2.1 The Confidentiality, Integrity and Availability of Information 13

2.2.2 Information Security Risks 14

2.2.3 Nature of Information Security Controls 14

2.3 Information Security Management Today 16

2.3.1 Information Security Risk Dimension 18
2.3.2 Information Security Policy Dimension 20
2.3.3 Information Security Awareness Dimension 21
2.4 International Standards for Information Security Management 23
2.5 Conclusion 26

3 ISM in Local Government 27
3.1 Introduction 27
3.2 Current Status of Information Security Management in Local Government 28
3.3 Initiatives in Local Government towards Better Information Security Management 29
3.3.1 Corporate Governance of ICT Policy Framework 30
3.3.2 The South African Local Government Association . . . 33
3.3.3 Municipal Corporate Governance of ICT Policy (MCG-ICTP) 34
3.3.4 Challenges that Local Governments Face with the Implementation 37
3.4 Criteria for Sound Information Security Management in Local Government 38
3.5 Conclusion 40

4 Research Approach 41
4.1 Introduction 41
4.2 Research Paradigm 42
4.3 Research Process 43
4.4 Research Process in Context 46
4.4.1 Phase 1: Analysis 47
4.4.2 Phase 2: Development 48
4.4.3 Phase 3: Refinement 49
4.4.4 Phase 4: Reflection 50
4.5 Research Methods 51
4.6 Conclusion 53

5 FISM in Local Government 54
5.1 Introduction 54

5.2 Part A: Developing FISM 55
5.2.1 Phase One: Analysis 55
5.2.2 Phase 2: Development 57
5.2.3 Phase 3: Refinement 58
5.3 Part B: Finalised FISM 63
5.3.1 Architecture for FISM 63
5.3.2 Process for FISM 65
5.4 Conclusion 68

6 Validation of FISM 69
6.1 Introduction 69
6.2 Data Collection 70
6.3 Data Analysis and Results 73
6.3.1 Results on the Scalability of FISM 73
6.3.2 Results on the Usability of FISM 73
6.3.3 Results on the Simplicity of FISM 74
6.3.4 Results on the Holistic Nature of FISM 75
6.4 Findings 77
6.5 Conclusion 79

7 Conclusion 80
7.1 Introduction 80
7.2 Summary of Findings 81
7.3 Meeting the Objectives 82
7.4 Summary of Contributions 86
7.4.1 Research Contribution: The Artefact 86
7.4.2 Methodological Contribution 87
7.4.3 Academic Publications 87
7.5 Future Research 88
7.6 Epilogue 88

References 90

Appendix A - MISP Example 94

Appendix B - Workshop Questionnaire 101

Appendix C - IST-Africa 2015 Publication **104**

Appendix D - IST-Africa 2016 Publication **115**

Appendix E - Journal of Public Administration (Under Review) **127**

List of Tables

1.1 List of Appendices 9

3.1 CGICTPF Deliverables and Deadlines 31
3.2 Municipal Capacity Categorisation 32
3.3 MCGICTP Deliverables and Deadlines 36

4.1 Principles for Design-Oriented IS Research 43
4.2 Design-based Research: Elements in Phases 45
4.3 Design-based Research Phase 1 47
4.4 Design-based Research Phase 2 48
4.5 Design-based Research Phase 3 49
4.6 Design-based Research Phase 4 50
4.7 Research Methods & Definitions 52

5.1 Elements of Phase 1: Position within Research Study 56
5.2 Elements of Phase 2: Position within Research Study 58
5.3 Elements of Phase 3: Position within Research Study 59

6.1 Description of Demographics of Workshop Attendees 70
6.2 Criterion Tested for by Questions of Questionnaire 72

List of Figures

1.1 Status of Information Security Controls in Local Government . 5

2.1 Information Security Competence Maturity Model 22

4.1 Design-Oriented IS Research Process 43
4.2 Design Research in Educational Technology Research 44
4.3 Integrated Research Process 46

5.1 Integrated Research Process Development of Framework . . . 55
5.2 Initial Draft Framework 58
5.3 Second Draft Framework (Architecture of Framework) 60
5.4 Third Draft Framework (Process of Framework) 62
5.5 Architecture for FISM 64
5.6 Process for FISM - Category Selection (Step 1) 66
5.7 Process for FISM - Control Selection (Step 2) 67
5.8 Process for FISM - ISPA Generation (Step 3) 67

6.1 Results of Question 4 73
6.2 Results of Question 6 74
6.3 Results of Question 1 74
6.4 Results of Question 7 75
6.5 Results of Question 3 75
6.6 Results of Question 5 76
6.7 Results of Question 2 76
6.8 Consolidated Questionnaire Results per Criterion 78

Chapter 1

Introduction

This chapter serves as the guide to the remainder of this research dissertation. In essence, this chapter provides the necessary background information to provide a sound context of this study. The context provided by this chapter includes the statement of the problem that the research study aims to address. In addition to stating the problem, this chapter also provides the objectives, both primary and secondary, which collectively contribute to addressing the problem at hand. The thesis statement provided reflects the core essence of this study. The scope and delineation of this study are also discussed in this chapter. This chapter also provides the roadmap to the remainder of the dissertation by describing the layout, before concluding the chapter.

1.1 Information Security Management and Local Government

In any contemporary enterprise, both public and private, information is arguably of critical importance to the success of the enterprise and thus, its value is immeasurable. The use and processing of such valuable information is significantly becoming more reliant on Information and Communication Technology (ICT) systems (Whitman & Mattord, 2012). This is due to the fast pace at which technology is evolving and its pervasiveness in modern enterprises. Thus, ICT is a major contributor to the effective execution of business processes in enterprises across the world (Ifinedo, 2012). Therefore, in light of the immense value of information, it is imperative to protect all information assets, including the systems that accommodate the information.

Governments in the African continent have realised this fact and are pursuing various avenues in an effort to optimise their use of ICT in order to enable effective service delivery to the local population (IST-Africa Initiative, 2015). This is definitely the case for the local government of South African. Considering the above mentioned, the rest of this chapter aims to briefly explain the structure of the South African government, determine the status of the use of ICT within local government and finally, motivate why information security management should be a key concern to local government.

1.1.1 Layout of Local Government within South Africa

South Africa is governed at three levels namely: nationally, provincially and locally as dictated by the Constitution, which is the supreme law in the country (Republic of South Africa, 1996). These three levels are interdependent and structured in a hierarchical manner.

The lowest level, which is the local government, is the closest link between the strategic decision making of the presidency and the general public. This level is where the strategic plans of government are exhibited at an operational level, in such a way that it is proverbially tangible to the public. Therefore, this study focuses solely on the local government level, as information security in this context, almost directly affects the public. The mandate of local government is fulfilled by means of municipalities. The Constitution states that the objectives of local government are (Republic of South Africa, 1996):

To provide democratic and accountable government for local communities To ensure the provision of services to communities in a sustainable manner To promote social and economic development To promote a safe and healthy environment To encourage the involvement of communities and community organisations in the matters of local government.

Due to the above-mentioned objectives, it is imperative for local government to use ICTs in a way that sustains and promotes these objectives. Furthermore, in addition to these objectives, the functions and responsibilities of municipalities are to provide various services to the local citizens. According to the Constitution Republic of South Africa (1996), some examples of these services are: electricity, water, sewage and sanitation, refuse removal, health services, public transport, library services and local tourism. In order to deliver these services, local government relies heavily on information being readily available. Considering the above, the following subsection will motivate why local government should embrace ICT in order to improve service delivery and business processes.

1.1.2 Role of ICT in Municipalities

Nowadays, all of the above-mentioned services are to some extent being rendered and enhanced by utilising ICTs. This statement is supported by the following extract from an official document of, the Corporate Governance of ICT Policy Framework, as it states, "The purpose of ICT is to enable the Public Service in its quest for service delivery" (Department: Public Service and Administration, 2012). Thus, ICT as a vital stepping-stone in assisting local government to achieve better service delivery is supported by the political leadership of the country. Therefore, it is undeniably imperative that local government applies due care in establishing effective governance of ICT.

The importance of the effective governance of ICT is due to the fact that local government relies heavily on information and related enabling technologies. The need to protect these informational resources properly is, therefore, inevitable to local government. The protection of information and related technologies is normally referred to as information security. When referring to information security, it is generally accepted that this term includes, not only the information itself but also the technologies and systems involved with information processing, usage and transmission (Whitman & Mattord, 2012).

Three key elements collectively contribute towards the safe keeping of information in the context of information security, confidentiality, integrity and availability. Gerber, Von Solms, and Overbeek (2001) define confidentiality as, "Confidentiality refers to the property that information is not made available or disclosed to unauthorised individuals, entities, or processes." The property of integrity aims to ensure that data is not altered or removed without the proper authorisation (Gerber et al., 2001). Availability requires that data be readily available upon demand by all authorised individuals, entities, or processes (Gerber et al., 2001).

Due to the complexity of the multifaceted process, that is information security, it is important that this process is properly managed, and this is usually conducted through a process of information security management. In order for local government to address information security management, it is worthwhile to refer to related internationally recognised standards and best practices for guidance. In the South African context, one of the leading codes of best practice for corporate governance is the King III Code (IoDSA, 2009).

The King III Code applies to enterprises across all sectors including the local government. It dedicates an entire chapter to promoting the proper and effective governance of ICT. This is due to the critical nature of the role it plays in supporting operational functions within an enterprise. In addition, the internationally recognised ISO/IEC 27000-set of standards directly addresses the management process of information security.

This process of managing information security is usually achieved by implementing an information security management system. An information security management system is defined in ISO/IEC 27000 (ISO/IEC 27000, 2012) as consisting of, "The policies, procedures, guidelines and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets." The following subsection will discuss the status of information security management within local government.

1.1.3 Importance of Information Security Management within Local Government

Information Security Management is a key aspect in the good governance of ICT. The King III Code supports this statement, as it states that information security, information management and information privacy must be properly addressed, in order to ensure that information assets are managed effectively (IoDSA, 2009).

The King III Code was published in 2009; this was the first instance that an entire chapter was dedicated towards ICT and its governance. However, the Presidential Review Commission already stated in 1998 that, "All ICT decisions should come from Senior Political and Managerial leadership and should not be delegated to technology specialists" (Presidential Commissioners, 1998). This was stated more than ten years prior to King's inclusion of this concept in his code.

Although the need, to properly govern the use of ICTs and the security of these systems is stressed by both strategic leadership and codes of best practice, little improvement has been made by local government in this regard. The Auditor-General of South Africa has highlighted this fact in his reports on the findings of both 2008/09 and 2009/10. In the 2012/13 findings again, the Auditor-General stated that, the status of information technology controls is concerning and municipalities are struggling to effectively implement the necessary measures to improve the security of ICTs (Auditor-General of South Africa, 2014). More than half of the municipalities were yet to design controls for information security management, and a further 12% had controls designed, but they struggled with the sustainable implementation thereof (Auditor-General of South Africa, 2014).

Another concerning fact is that 68% did not have any controls designed to address the aspect of user access management, a core element of information security management (Auditor-General of South Africa, 2014). In the most recent reports of the Auditor-General for the financial year of 2013/14, it is clear that local government has made little improvement in securing informational assets. Figure 1.1 below shows the status of these controls as they currently reside in comparison with the previous year's findings (Auditor-General of South Africa, 2014).

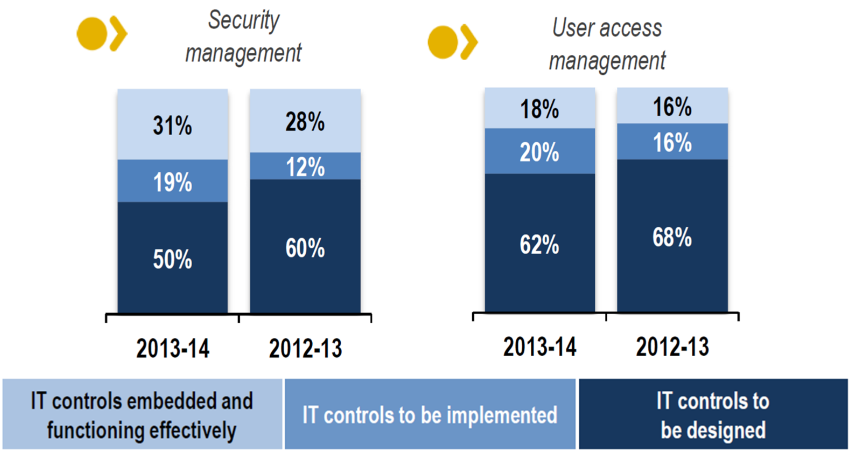


Figure 1.1: Status of Information Security Controls in Local Government

Although some improvement is evident, the majority of local governments do not have effectively functioning controls that address information security. The following section will aim to define the problem, taking into consideration the above mentioned information.

1.2 Current Challenges of Local Government

From the previous section, it is clear that the general management of the security aspects of information and related technologies are not addressed properly in most South African municipalities. This is a concerning situation as highly valuable and sensitive information is processed in high quantities by municipalities and the loss in the confidentiality, privacy and integrity thereof could result in disastrous consequences.

Thus, the problem statement that this research aims to address is the following:

It is in the best interest of local government in South Africa to protect all information assets, including the systems that accommodate the information. However, most municipalities are failing to implement effective information security management.

1.3 Thesis Statement

The core message and challenge conveyed in this research study is captured in the following thesis statement:

Information is critical to all business functions within local government. This implicates the ICT systems that accommodate the information and thus, effective information security management is vital in ensuring the security of all information assets within local government. In so doing, local government can ensure more effective service delivery to the local communities.

This thesis statement is the perfect-world manifestation of what the researcher would ideally want to achieve through this research study. When this vision captured in the thesis statement comes to full fruition, the problem that this study addresses would truly have been resolved.

1.4 Research Objectives

In accomplishing the following objectives, this research study aims to address the problem described previously and provide local government with a practical solution for the management of their information security.

Primary Objective:
To formulate a framework that will assist local government in South Africa, to implement sound information security management effectively.

In order to accomplish the menial task of formulating such a framework, the secondary objectives divide the primary objective into manageable portions. Thus, the secondary objectives collectively contribute to the achievement of the primary objective.

Secondary Objectives:

- To determine the key contributing factors that hinder local government in implementing effective information security management
- To study standards and best practices to determine the key components of information security management that are relevant to local government
- To articulate a holistic approach by which local government can improve and adapt their individual information security management to align with their requirements

1.5 Scope and Delineation

This study focuses specifically on local government which includes district and local municipalities and not necessarily on metropolitan municipalities. The reason for this is that the main goal of the study is to assist municipalities which are categorised as poor resource, low capacity municipalities, which does not necessarily apply to metropolitan municipalities. Furthermore, although this study is focused specifically on the South African context, it can easily be generalised to similar scenarios around the world as it is based on the principles and aspects from international standards and best practices.

1.6 Research Approach

As argued prior to the problem statement, local government is faced with a very real problem in that it is mostly beset with inadequate controls for the management of information security. This real-world problem was addressed by designing a framework for effective information security management in local government. This framework was designed to be in the form of an artefact. Design-oriented information systems research was identified as the logical research paradigm. An extensive, detailed discussion on design-oriented information systems research and the research process and methods followed, will be espoused in Chapter 4.

1.7 Layout of Dissertation

The layout of this dissertation is comprised of seven chapters. The individual chapters serve a specific purpose and are ordered to provide a logical unit.

The research study is introduced in Chapter 1, by firstly describing the topic area and related background information. Consequently, the research problem is described and stated, along with the objectives that aim to address the problem. The thesis statement describes the essence of the research study.

The second chapter provides the detail of the topic area of information security management. It looks at common practice within modern day information security management and its core components.

After which, information security management is contextualised and discussed from the perspective of local government in Chapter 3. The unique challenges to local government are also discussed here and criteria to address those challenges are argued.

Within Chapter 4, the research approach of this study is described. This is done by firstly, describing the paradigm and the research process. This chapter concludes by describing the research methods used throughout the study.

The fifth chapter describes the development of the artefact of this study which is in the form of a framework. This development of the framework is described by discussing how the research process was followed in order to formulate the framework. Consequently, the finalised version of the framework called Framework Towards Information Security Management (FISM) is also described in Chapter 5.

Chapter 6 provides detail on the validation exercise conducted in order to measure to what extent the framework adheres to the criteria as seen in Chapter 3.

Finally, Chapter 7 draws conclusions stemming from all preceding chapters and reports on the achievement of the objectives of this study.

Table 1.1: List of Appendices

NAME	DESCRIPTION
Appendix A	Example of Municipal Information Security Policy (MISP)
Appendix B	Workshop Questionnaire
Appendix C	IST-Africa Conference Paper 2015 (Published) - Better Information Security Management in Municipalities
Appendix D	IST-Africa Conference Paper 2016 (Published) - Information Security Management in Local Government
Appendix E	Journal of Public Administration (JoPA - submitted) - A Self-Help Approach to Information Security Management in Local Government

In addition to the above mentioned chapters, several appendices are added at the end of this dissertation to supplement it with additional information as necessary. Table 1.1 provides the details of the appendices included as part of this dissertation.

1.8 Conclusion

This chapter introduces the research study and the topic area. The topic area is structured in three parts. The first of these three parts, described the layout of the South African government and its structures, especially in the context of local government. The second part highlighted the importance and role of ICT within local government. The third and final part described the topic of information security management and its status in local government. This discussion on the topic area and the specific context of this study served as the prelude to the problem statement of this study.

Consequently, this chapter provides a thesis statement for this study, which captures the essence of this study and the its vision. After this, the study was delineated and its scope defined, before discussing the research objectives which aim to address the problem at hand. Furthermore, the research approach followed by this study was briefly summarised, before detailing the layout of the research dissertation.

Chapter 2

Contemporary Information Security Management

This chapter aims to provide the foundational context, from literature, for the contemporary approach to information security management. It commences by examining the position of ICT within the modern enterprise, followed by highlighting the position of information security, related to ICT. It then continues by discussing various standards and best practices on information security that can be used as guidance towards sound information security practices. The chapter then continues to discuss the key elements, again from literature, to incorporate when managing information security.

2.1 Introduction

In any modern day enterprise, ICT is of the utmost importance. As Carr (2003) hints in his somewhat controversial paper, the mere utilisation of ICT in an enterprise provides little advantage over competitors. He argues that ICT is rather an indispensable commodity for conducting business, much like electricity. The technological boom of the modern era, stemming from the development of the microprocessor in the late 1960s, is largely responsible for the rise in importance of ICT. The reason for this is that many technologies, such as desktop computers, local and wide area networks and the Internet were invented after the introduction of the microprocessor (Carr, 2003). All of these technologies are largely commonplace in enterprises of all types and are heavily relied upon by operational processes.

However, the heavy reliance of operational processes in an enterprise on ICT is more deeply rooted than the ICT itself. The information that is stored, processed and transmitted via the ICT systems, is what is ultimately of most value to the enterprise (Whitman & Mattord, 2012). Furthermore, the information can be seen as the heart of the enterprise and the lifeblood to all of its business functions, as enterprises rely on information for communication purposes, process support and decision making (Belanger & van Slyke, 2012).

Thus, it can be argued that the real value of ICT in the modern era is not merely in the presence of ICT within an enterprise; but rather in the way that it is used to communicate information to influence both, decision making and how it provides support for operational processes. Taking this into consideration, it is fair to say that information and related resources, such as ICT, is a crucial asset within any enterprise today.

The significant importance of information and related ICT resources gives rise to the need to keep such assets safe from danger. Therefore, due to its importance, it is critically important for enterprises to protect their information and related ICT resources. The protection of information and related resources is commonly referred to as information security.

Thus, this chapter discusses the contemporary approach to information security management and the core components that need to be incorporated by an enterprise to address its information and ICT risks. The chapter will be structured as follows, firstly, what information security entails; secondly, discussing the management of information security and the multiple dimensions that it consists of. Thirdly, the chapter will discuss several international standards that provide guidance in the implementation of information security management before it is concluded.

2.2 The Security of Information and Related Resources

There are many factors to consider when protecting information and related resources, by the formal process of information security. First, it is important to protect information throughout all of its various states. These states in which information should be protected include: while it is in storage, while it is being processed or used, as well as while it is in transit (McCumber, 1991; Whitman & Mattord, 2012). This principle of information security applies to information of all types, which includes electronic or digital information, also known as 'soft' information and printed media, referred to as 'hard' information.

2.2.1 The Confidentiality, Integrity and Availability of Information

In addition, information security aims to preserve the Confidentiality, Integrity and Availability (CIA) of information (Fuchs, Pernul, & Sandhu, 2011; ISO/IEC 27000, 2012; Posthumus & Von Solms, 2004; Whitman & Mattord, 2012). These three properties or characteristics of information should be preserved across all of the information states mentioned previously. The confidentiality of information can be defined as being the property that ensures that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO/IEC 27000, 2012). Integrity, on the other hand, is said to be the property that aims to ensure and protect the accuracy and completeness of information assets (ISO/IEC 27000, 2012). Finally, availability is the property of information being accessible and usable upon demand by an authorised individual, entity or process (ISO/IEC 27000, 2012).

With this in mind, it can be argued that collectively, when protected properly, this CIA of information ensures to a large extent that the information and related resources of an enterprise are free from danger of being lost, stolen or misused (Gerber & Von Solms, 2001). Although these three properties of information, primarily constitute information security, other properties can also be involved such as; authenticity, accountability, non-repudiation and reliability (ISO/IEC 27000, 2012). Furthermore, when implementing information security, threats and vulnerabilities to information and related resources, as well as the impact of vulnerabilities being exposed by threats, have to be mitigated.

2.2.2 Information Security Risks

A threat is said to be the potential cause of an unwanted incident, which may result in harm to a system or enterprise (ISO/IEC 27002, 2013). While, a vulnerability is a weakness of an information resource or control, which can be exploited by one or more threats (ISO/IEC 27000, 2012). Finally, incidents where these vulnerabilities are exploited by threats can have perilous consequences for an enterprise. Thus, the impact of such incidents also has to be carefully considered when addressing information security issues.

These factors, vulnerabilities, threats and impact of information security incidents, are essentially what constitute an information security risk. These risks have to be treated satisfactorily in order to safeguard or protect information (Gerber & Von Solms, 2001). Thus, information security controls serve this purpose and are implemented to reduce the likelihood of such incidents occurring and/or reducing the consequence also referred to as impact, of such an incident to an acceptable level. Information security controls or safeguards, are therefore introduced as a treatment to associated security risks.

2.2.3 Nature of Information Security Controls

Information security controls, that treat these information security risks, can take many forms, including policies, procedures, guidelines, practices or organisational structures (ISO/IEC 27000, 2012). These controls can also vary in nature, ranging from administrative, technical, physical, management or legal controls (ISO/IEC 27000, 2012). For the purpose of this research, however, controls will be referred to in three main categories; which are operational, physical, and technological controls. Operational controls in the context of this study are a combination of administrative and managerial controls; while legal considerations will feature in the following section. Thus, operational controls aim to provide processes that mostly address the human aspect of information security.

This human aspect of information security essentially focuses on influencing the behaviour of humans when interacting with information and related resources (Furnell & Clarke, 2012; Sohrabi Safa, Von Solms, & Furnell, 2016). The need for the ICT systems to be protected by means of physical and technological controls, in order to indirectly protect the information on it, has long been an area of unquestionable importance and prominence within the information security community. However, the human aspect of information security has only become a prominent topic in the global research community in recent years and has since gained notoriety quickly (Furnell & Clarke, 2012).

Technological controls have long been the primary focus of information security practices and have been the subject of immense financial investment in the past, by enterprises across the world (Kayworth & Whitten, 2010). Such technological controls include the installation of firewalls, anti-virus software, anti-spyware, anti-malware, the backing up of information, encryption and much more (Ifinedo, 2012; Sohrabi Safa et al., 2016). Furthermore, such technological controls are mostly aimed at protecting electronic information and the ICT systems or software.

Physical controls, however, are aimed at protecting the ICT infrastructure itself and for restricting the physical access of unauthorised persons to information and related resources; which can also include the physical premises of an enterprise. These physical controls also extend beyond the electronic scope of technology-based controls, to the protection of printed information.

As mentioned before, in recent years the research community has been calling and advocating for a more balanced approach to information security, that addresses both operational, as well as technological and physical security issues. Furnell and Clarke (2012), argue that although humans represent a key part of information security achievement, they are often the weakest link and cause for vulnerability. Therefore, information security controls of an operational nature, which involve the human aspect of security, aim to positively influence human behaviour when handling information and in so doing, attempt to alleviate the risk that humans pose to information and related resources.

When influencing human behaviour to be acceptable, in terms of information security, the ideal result is that the people that handle the information perform security tasks almost subconsciously, without having to pay careful attention to executing it properly. When people are this well-trained, educated and security aware, it is argued by Thomson and Von Solms (2006), that information security obedience and thus, acceptable behaviour is part of the information security culture of the enterprise.

Security concerns of a technological and physical nature, and the operational issues associated with influencing human information security behaviour are addressed by identifying and implementing a comprehensive set of suitable security controls that is specific to the needs of the enterprise. The identification of such a set of suitable controls to treat related risks requires that these risks should be properly assessed. Furthermore, the implementation of security controls is a complex undertaking; which requires users to be educated regarding their role in the protection of information resources, in order for the controls to be effective.

In essence, all of the above mentioned information highlights some of the numerous core factors that need to be considered when addressing information security. In addition to these basic principles of information security, there are several dimensions that have to be incorporated into security practices. Thus, this added complexity adds to the fact that information security should be an informed and well-structured undertaking if it is to be effective. Ultimately, this calls for the sound management of the information security process in a comprehensive and formalised management process. This overarching management process is commonly referred to as information security management.

2.3 Information Security Management Today

Information security management, like any other management process, should typically follow a top-to-bottom approach. This is supported by Von Solms and Von Solms (2004), as they argue that information security is a corporate governance responsibility, which lies with the most senior management of an enterprise. Thus, information security should be managed with a clear vision and objective which it seeks to satisfy, as communicated by senior management.

These objectives should be identified while taking into consideration, that the process of managing information security is a complex and multi-dimensional process. Each of the many dimensions of information security should be carefully considered when implementing information security management, in order to avoid implementing a lop-sided management process (Von Solms & Von Solms, 2004); which is ultimately bound to fail.

Von Solms and Von Solms (2004), further argue that the exact number of dimensions and their precise content is not the most important issue, but rather the understanding that information security is, in fact, a multi-dimensional discipline and that the various dimensions collectively contribute towards the protection of information and related resources. In their paper, they state that the following dimensions can be identified without much difficulty:

- *The Corporate Governance Dimension*
- *The Organisational Dimension*
- *The Policy Dimension*
- *The Best Practice Dimension*
- *The Ethical Dimension*
- *The Certification Dimension*
- *The Legal dimension*
- *The Insurance Dimension*
- *The Personnel/Human Dimension*
- *The Awareness Dimension*
- *The Technical Dimension*
- *The Measurement/Metrics (Compliance monitoring/Real-time IT audit) Dimension*
- *The Audit Dimension*

Although all of these dimensions can rightly be argued to be of critical importance to the success of any information security management undertaking, three of them will be discussed in more detail as they are core to the scope of this research. The three dimensions that will be discussed in more detail are the Risk Dimension, the Policy Dimension and the Awareness Dimension.

The Risk Dimension is not explicitly listed by Von Solms and Von Solms (2004); they do, however, argue that there is no 'silver bullet' or one -size-fits-all solution for information security. This subsequently implies that, every enterprise should implement a specially tailored approach to information security unique to the needs of the enterprise, addressing risks to its information and related resources. Thus, some form of risk assessment exercise should help to identify the risks that need to be addressed; which will, in turn, ensure that the information resources of an enterprise are optimally protected.

2.3.1 Information Security Risk Dimension

Information security risk considers the potential incident of one or more threats exploiting a vulnerability of an information resource, the likelihood of such incidents occurring and the impact they might have when they do in fact occur (ISO/IEC 27000, 2012). In most cases within information security, the physical, technical and operational issues that manifest within an enterprise are addressed through the introduction of controls, to mitigate related risks. This implementation of controls to mitigate information security risks is commonly referred to as risk treatment.

However, before an enterprise can begin to treat any of its information related risks, the information security risk environment of the enterprise has to be properly assessed (ISO/IEC 27005, 2011). The activity of information security risk assessment is generally comprised of three parts. The first of these is the process of risk identification (ISO/IEC 27005, 2011). Once information security risks have been identified, the second part of assessing the risk environment is to analyse the identified risks (ISO/IEC 27005, 2011). Part of this risk analysis process is to comprehend the identified risks and to determine the level of urgency that each risk has to be addressed with; also referred to simply as the level of risk (ISO/IEC 27000, 2012). Finally, information security risks have to be evaluated by comparing the results of the risk analysis process with certain predetermined risk criteria specific to the enterprise. This process of risk evaluation serves the purpose of determining whether a risk is acceptable, tolerable or whether the risk has to be treated (ISO/IEC 27000, 2012).

As mentioned before, these three processes of identification, analysis and evaluation of information security risks, collectively contribute to the assessment of information risks. This activity of risk assessment has to be repeated continuously to address new threats and vulnerabilities as well as to cater for risks that result from changes in the environment, systems and infrastructure. However, the assessment of information security risk only categorises identified risks according to their potential to cause harm to the enterprise if realised. These risks, once assessed, still need to be mitigated to an acceptable level.

The formal activity of risk treatment serves the purpose of mitigating information security risks upon the completion of a satisfactory assessment. Within this activity, information security risks can be treated in numerous ways, as stated in ISO/IEC 27005 and includes (ISO/IEC 27005, 2011):

- Risk modification: Involves the introduction, removal or alteration of controls to the end that the residual risk is at an acceptable level upon reassessment
- Risk retention: The decision to wilfully retain a risk, without taking any further action towards mitigating the risk
- Risk avoidance: When action is taken to avoid the activity or condition that gives rise to the risk
- Risk sharing: When risk is shared with other parties in the most effective way

The outcome of treating an information security risk should be evaluated upon completion to determine whether or not the treatment administered, reduced or altered the particular risk to an acceptable level. As mentioned before, information security controls are implemented in order to treat these risks and mitigate them to an acceptable level. However, information security controls have to be properly communicated to all internal or external information users of an enterprise. These controls are most effectively portrayed in a collection of information security policies, which calls for the following subsection to discuss the information security policy dimension.

2.3.2 Information Security Policy Dimension

The objectives for information security should align with the corporate objectives of the enterprise, to ensure that information best supports the operational processes within the enterprise. In addition to the clear objectives for information security mentioned before, managing information security and related risks, needs the absolute commitment of senior members of management for it to be successful (Von Solms & Von Solms, 2004). This mission-critical commitment and objectives from senior management for information security should typically be communicated via a corporate information security policy, which is the basis of any successful attempt to manage information security (Cosic & Boban, 2010; Von Solms & Von Solms, 2004).

This corporate information security policy provides the vision for information security within the enterprise and is strategic in nature. Thus, such a corporate information security policy should be conceptual, reasonably generic and static; rather than containing much detail about the current business landscape or containing detail about technical issues (Von Solms & Von Solms, 2004). Although this policy should remain fairly static for the most part, it should, however, be reviewed regularly and adjusted when necessary, to ensure that it stays relevant. However, due to the lack of technical detail provided by this policy, it should be supplemented with sufficient secondary policies and procedures that provide the needed support in this regard (Von Solms & Von Solms, 2004).

The second tier of policies for information security is also referred to as secondary, issue-specific or supporting policies and is typically more detailed, specific and dynamic than the high level corporate information security policy. These supporting policies also take into account both the current technological or business landscape, and both the current and future projects within the enterprise (Von Solms & Von Solms, 2004). Furthermore, these supporting information security policies are often dedicated to addressing a single topic such as internet or email usage, information classification, access control or network security and as such, they are often referred to as issue-specific (ISO/IEC 27002, 2013; Von Solms & Von Solms, 2004). In addressing these various topics, the supporting information security policies aim to address the technical, physical and operational issues of information security within the enterprise. Subsequently, by introducing these policies, an enterprise sets the goal to treat the unique and specific risks related to its information resources, in order to mitigate the risks to an acceptable level.

However, merely stipulating and communicating the objectives and vision of the enterprise for information security to the information users of the enterprise, from a strategic corporate policy right down to the operational and technological issues of the supporting policies, is not enough to ensure that the desired information security behaviour will be manifested (Von Solms & Von Solms, 2004). Thus, the enterprise information users have to be reminded, trained and educated continually for the various policies to have the most effective impact in influencing or dictating human behaviour in issues of information security (Von Solms & Von Solms, 2004).

2.3.3 Information Security Awareness Dimension

Thomson and Von Solms (2006), proposed a model by which employees of an enterprise can become skilled in information security practices. The model requires an information security awareness programme as a basis. It is based on the 1982 Conscious Competence Learning Model by Howell. Howell and Fleishman Howell and Fleishman (1982), argue that there are four stages of competency in accomplishing a task or when learning a new skill. Thomson and Von Solms (2006), argue that information security awareness, training and education can guide an individual through these four stages of competency. This is depicted in Figure 2.1, with information security obedience being the culmination of progressing through these stages.

The manifestation of information security obedience will prove very crucial to effective information security, as it should assist to substantially mitigate risks to information resources, where human behaviour is involved. The instructions for acceptable behaviour towards information security that have to be obeyed, should be communicated via various policies, procedures and other official enterprise documentation.

Thus, in order to attain information security obedience, all information users have to be made aware of these policies on a regular basis. Furthermore, training is needed to provide the necessary skills to execute the required tasks to safeguard the information resources of the enterprise. Finally, education provides further insight and a deeper understanding of the necessary terms and concepts within information security.

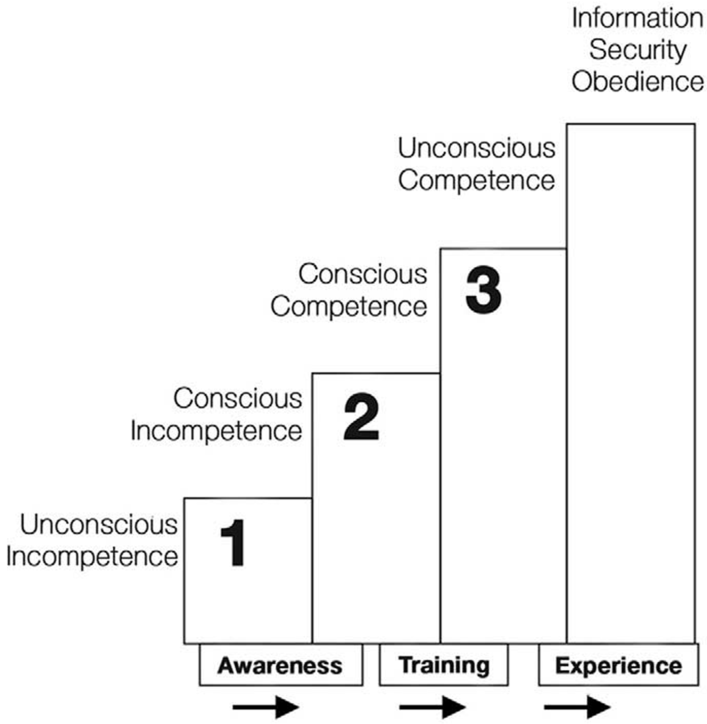


Figure 2.1: Information Security Competence Maturity Model

In summary, a collection of logically structured policies is the basis and point of reference for any efforts towards managing information security within an enterprise (Cosic & Boban, 2010; Von Solms & Von Solms, 2004). However, the information security policies of an enterprise should be designed to address the specific information security risks of the enterprise, as per a risk assessment exercise. Assessing organisational information and ICT risks is normally applied on two tiers. Firstly, at a high level to influence the drafting of the corporate information security policy. Secondly, at a lower, more detailed level as dictated by the Corporate Information Security Policy (CISP). Furthermore, a proper information security awareness programme is a critical success factor for such policies to have the desired effect within the enterprise.

Therefore, managing information security should be addressed by way of a formal management system, structured to incorporate the various dimensions of information security with careful attention to detail; while at the same time catering for the dynamic and ever-changing nature of the information security landscape. Such an Information Security Management System (ISMS) may potentially seem like a daunting undertaking for the senior management of an enterprise. However, there are international standards that provide sound guidance for information security management and the implementation of an ISMS. Thus, the best practice dimension of information security should be incorporated to ensure that an enterprise not only has an ISMS that is relevant to its own needs but that it is at least on par with the information security implementations of the global industry it operates within.

2.4 International Standards for Information Security Management

The most prominent standards for information security today, are provided by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). These two organisations form the specialised system for worldwide standardisation across most industries. The ISO/IEC collection of international standards, as they are commonly referred to, contain a group of standards devoted completely to information security and its management and are within the 27000-range (ISO/IEC 27000, 2012).

This information security oriented group of standards is collectively referred to as the ISMS-family of standards. The first of these ISMS standards is the ISO/IEC 27000 standard; which serves as an introduction to and provides an overview of the family as a whole, as well as, defines terms and vocabulary related to the other standards in the family (ISO/IEC 27000, 2012).

Within the ISO/IEC 27000 standard, the focus is fittingly placed on defining the concept of an ISMS and its related processes. An ISMS is said to be a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security of an enterprise to achieve its business objectives (ISO/IEC 27000, 2012). These processes are critical to the success of managing information security within an enterprise. The monitoring, reviewing and improvement of the ISMS should be a never-ending cycle to ensure that the information resource of the enterprise is optimally protected at all times. Furthermore, an ISMS consists of policies, procedures, guidelines, and associated resources and activities;

which are to be managed collectively by an enterprise, in the pursuit of securing its information resources (ISO/IEC 27000, 2012). In essence, an ISMS is a comprehensive framework by which an enterprise manages its information risks to ensure that its information resources are adequately protected. Ultimately, the main purpose of the ISO/IEC 27000, is to provide the reader with a sound understanding of an ISMS, its importance and introducing the reader to related processes and activities.

However, within the ISO/IEC 27001 standard, more intricate details about the various processes required for, and involved with, the implementation of an ISMS are provided and they can be easily deduced from the title of this standard - "Information security management systems - Requirements". When implementing an ISMS, an enterprise should thoroughly evaluate its needs and objectives for information security and scale its ISMS implementation accordingly (ISO/IEC 27001, 2013). The ISO/IEC 27001 standard provides extensive detail for the various requirements for an ISMS, including (ISO/IEC 27001, 2013):

- Understanding the context of the enterprise, which includes determining the scope of the ISMS
- Leadership commitment and policy, including the assignment of roles and responsibilities for information security
- Planning for the ISMS, especially regarding the assessment and treatment of information security risks
- Support for the ISMS, in terms of the competence and awareness in the enterprise related to the ISMS and resource allocation for implementing and maintaining the ISMS, amongst others
- Operation of the ISMS - addressing planning and risk issues at an operational level
- Performance evaluation which includes measurements, review and assessment of the ISMS, with the eventual goal of continual improvement
- Improvement of the ISMS, detailing the improvement process and approach for an ISMS

The ISO/IEC 27001 standard, largely addresses issues that are of a strategic nature, related to the management process itself; whereas, guidance for the actual implementation of controls within the ISMS to treat information risks is found in a further standard in the 27000 series.

The standard that provides this guidance for implementing information security controls, is the ISO/IEC 27002 standard. The latest revision of this document was released in 2013 and consists of 114 security controls; which are divided logically into 35 security categories, with each category containing one or more controls (ISO/IEC 27002, 2013). The security categories of this standard are also presented in 14 logical groupings called clauses (ISO/IEC 27002, 2013). The security controls presented by this standard are a comprehensive collection of commonly accepted controls, which address the multiple dimensions of information security and a wide range of information risks. Thus, an enterprise is free to take these security controls and implement them at face value, or if needed - other controls can be designed to address the needs of the enterprise that are unique and specific to its operating environment (ISO/IEC 27002, 2013). However, the security controls within the ISO/IEC 27002 standard are a sound starting point and foundation for an enterprise to build its ISMS on. Interestingly, information security policies are largely the core of this standard and most security controls relate to this somehow.

The implementation of security controls within an ISMS, however, should address the information risks of the enterprise. Thus, guidance should also be sought for the proper assessment of risks and their treatment based on the results of the assessment. Such guidance, for information security risk management, can be attained by consulting the ISO/IEC 27005 standard; which is a crucial component of any ISMS to ensure that the ISMS is relevant to the needs of the enterprise (ISO/IEC 27005, 2011).

It is important to note that the ISO/IEC 27000 family of standards are not limited to the few standards that are discussed in this section but include several more standards that will not be discussed here. All of the standards discussed in this section, collectively contribute towards the implementation of an ISMS. These standards are readily available and in most cases require little to no adaptations, as they are applicable in enterprises of any shape or size. Furthermore, with an effective ISMS implemented within an enterprise, the safety of its information resources should not be of great concern. Therefore, to ensure the prolonged security of information resources, the ISMS of an enterprise should be continually maintained and improved.

2.5 Conclusion

This chapter set out to provide the foundational context, for contemporary information security management. It was argued that information is a critical enabler for business processes. In the modern enterprise, business processes rely heavily on ICT systems to process such information. Therefore, it is undeniable that all information assets should be adequately protected as they are a growing concern globally.

In order to protect information resources within an enterprise, information risks have to be identified, assessed and treated to an acceptable level. The treatment of these information security risks is done by identifying and implementing a set of suitable security controls.

An ISMS is a comprehensive framework or umbrella, under which the above processes of information security are executed. Some of the key components that form part of an ISMS are clear objectives for information security, a multi-tier collection of policies for information security, an information security awareness programme and finally, a continual effort to improve the ISMS by monitoring its performance.

The following chapter will look at information security management through the lens of local government within South Africa.

Chapter 3

Information Security Management in Local Government

This chapter aims to discuss information security management in the context of local government, as the contribution of this research is aimed at assisting local government, in this regard. The chapter commences by discussing the current status of information security and its management, within local government; followed by a discussion on the various initiatives within local government to remedy the cause for concern. It then continues by discussing the unique challenges within the operating environment of local government that have to be overcome in order to make significant progress in information security practices. The chapter then continues to argue towards principles that have to be incorporated into any contribution for local government for information security management, to address their unique challenges.

3.1 Introduction

In the previous chapter, it was argued that sound information security management is essential to provide adequate protection to information and related ICT resources. Furthermore, the importance of information and the growing need to properly protect it is applicable to enterprises of all shapes and sizes, ranging from the smallest to the largest, both public and private in nature regardless of capacity. Therefore, local government is also required to protect its information and related ICT resources, just like any other enterprise. This mandate to protect information and manage related privacy issues, in the South African context, stems from the King III Report (IoDSA, 2009); which is regarded as the blueprint for all matters of corporate governance, including information security as a subset of ICT governance. The King III Report is held to such a high esteem that it is expected of enterprises to either comply with the principles therein or else explain why they can or do not comply. Consequently, local government needs to protect its information and related resources through a process of information security management.

The aim of this chapter is, therefore, to discuss the current status of information security management within local government. The chapter will also analyse the operating landscape of local government and the unique challenges that accompany it. The chapter will end by arguing towards certain criteria that need to be addressed in assisting local government to help themselves towards implementing sound information security management. These criteria will be core to define and argue towards the framework that forms the main contribution of this research study.

3.2 Current Status of Information Security Management in Local Government

The current status of information security management in local government, along with many other issues and concerns, is clearly portrayed by the annual reports of the AGSA. These reports reveal the findings of annual audits of local government to the public, which promotes transparency between local government and the communities they serve. The AGSA reports are a reputable and independent source of analysis of the current status of affairs in local government (AGSA, 2015). It is necessary to note that the reports highlight ICT as a key risk area that needs to be addressed by local government.

Furthermore, there are four control areas within ICT that need to be addressed, which are; ICT governance, information security management, user access management and ICT service continuity, respectively (Auditor-

General of South Africa, 2015). This research study will only focus on the controls for information security management. However, although user access management and information security management are separately reported on by the AGSA, for the purpose of this research study they will be seen as one to align with commonly accepted best practice (ISO/IEC 27002, 2013).

In recent years, the AGSA reports indicate a slight improvement in information security management controls. However, this improvement is really slow and is therefore deemed as highly unsatisfactory (Auditor-General of South Africa, 2015). This is clearly depicted in Figure 1.1, as the amount of local government entities that have embedded and functioning controls for information security management has only risen by 3% to 31% during the last financial period (Auditor-General of South Africa, 2015). This is of concern, as it leaves local government with more than two-thirds of its entities stranded with controls that are either, not designed at all, or designed but not properly implemented and this is also depicted in Figure 1.1 (Auditor-General of South Africa, 2015).

Thus, it is clear that the current status of information security management practices in local government is a matter of concern. In spite of this, local government and related government departments have not been idle in their attempt to improve the implementation of information security management controls. A closer look will now be taken at various initiatives with regard to sound information security management practices within local government.

3.3 Initiatives in Local Government towards Better Information Security Management

The critical importance of information and related ICT resources is nothing new to local government in South Africa. This is reflected in the 1998 Presidential Review Commission (PRC) report, in chapter 6 section 2.2.1, which states that, "ICT will be aligned with Government Business Goals and will be a change agent to create responsive, result oriented, value added Public Service" (Presidential Commissioners, 1998). Thus, utilising ICT and the information it processes, as an enabler for service delivery is what local government should be striving for, according to a mandate from senior political leadership. The AGSA, however, pointed out in 2008/09 and again in 2009/10, that local governments strides towards this ideal eventuality was mostly stagnant for little over a decade (Department: Public Service and Administration, 2012).

It is very likely that this bold statement of the AGSA, about a seemingly forgotten mandate, sent a wave of panic through the ranks of local government, which had the desired effect of provoking it to take action. The AGSA recommended that a government-wide governance of ICT Framework be put in place as part of a national ICT strategy to govern ICT risks. All of the above mentioned, to a large extent, contributed collectively to the drafting of the Corporate Governance of ICT Policy Framework (CGICTPF), by the Department of Public Service and Administration (DPSA) in 2012.

3.3.1 Corporate Governance of ICT Policy Framework

This CGICTPF, as mentioned before, was drafted so that it be implemented as part of a government-wide initiative to improve the use of ICT in delivering valuable services to the general public. This CGICTPF aims to provide guidance that will inform proper governance structures, assignment of roles and responsibilities and the implementation of controls to mitigate information risks related to the use of ICT (Department: Public Service and Administration, 2012). In terms of scope, however, this document applies to all levels of government, across all departments of government and thus, does not address the very unique operating environment of local government.

The CGICTPF introduced an implementation timeline where certain deliverables had to be met at various deadlines. Table 3.1, depicts these deliverables and the deadlines that form the three-phased implementation approach of the CGICTPF (Department: Public Service and Administration, 2012).

Through the timelines provided by the CGICTPF in Table 3.1, the entire South African government should have been boasting a fully functional and effective set of controls for ICT, its governance and various ICT related functions, for well over a year already (Department: Public Service and Administration, 2012). However, it is clear from the AGSA annual audit findings that this is not the case in local government, as they still face many challenges in this regard, particularly with information security management

Table 3.1: CGICTPF Deliverables and Deadlines

PHASE	**Phase Deadline:**	**Deliverable Description:**
Phase 1	March 2014	Approved Governance of ICT Charter
		Governance Champion
		Appointed Government Information Technology Officer (GITO)
		ICT Manager Appointed
		Approved Risk Management Policy
		Approved ICT Management Framework
		Approved ICT Security Policy
		Approved ICT Continuity Policy
		Approved Internal Audit Plan
		Approved Portfolio Management Framework
Phase 2	March 2015	Approved ICT Strategic Plan
		Approved ICT Migration Plan
		Approved First Iteration of Enterprise Architecture
		Approved ICT Procurement Strategy
		Approved ICT Annual Performance Plan
Phase 3	April 2015 onwards	Corporate Governance of and Governance of ICT must demonstrate measurable improvement

(Auditor-General of South Africa, 2015).

Although the CGICTPF focuses on the governance of ICT in general, it does have a deliverable in phase 1 that is oriented towards information security management, an ICT Security Policy (Department: Public Service and Administration, 2012). This ICT Security Policy is the only mention of information security related issues throughout the CGICTPF. However, according to international standards and common best practice, this single ICT Security Policy prescribed by the CGICTPF is insufficient in addressing information security management comprehensively. This is substantiated in the previous chapter, as it motivates a multi-level hierarchy of policies as a best practice to address information security risks. Thus, the CGICTPF provides little detail to the resolution of information security management issues within local government.

From the local government perspective, failure to address information security management issues was not the only pitfall of the CGICTPF, as it was also deemed too complex, for implementation in local government. Local government is largely incapable of attaining the desired results within the timelines of the CGICTPF, due to capacity and resource constraints, as well as the fact that every municipality functions independently and most probably differently than its neighbouring municipalities. This is highlighted by the South African Local Government Association (SALGA) as they state that, when it comes to ICTs in municipalities:

- Operate in a very isolated non-uniform manner
- Are ill-prepared to face the required ICT resource, skill and budget constraints
- Have limited access to or support from other spheres of government and are often left to the mercy of the market

(SALGA, 2012)

Furthermore, municipalities are categorised by the National Treasury according to their financial management capacity as; high, medium or low capacity. This value represents the resource availability within a municipality and its ability to raise revenue. In addition to this, municipalities are categorised further according to fiscal capacity as either poor, adequate or resource rich. When these two possible categorisations are combined, municipalities fall into one of five categories, as depicted in Table 3.2 (SALGA, 2012).

Table 3.2: Municipal Capacity Categorisation

Financial Management Capacity	**Fiscal Capacity**
High Capacity	Rich in Resources
Medium Capacity	Adequate Resources
Medium Capacity	Poor Resources
Low Capacity	Adequate Resources
Low Capacity	Poor Resources

However, a concerning fact is that the last category of poor resource - low capacity, represents 30% of municipalities in South Africa (SALGA, 2012).

Thus, the framework for local government, which forms the contribution of this research, needs to scale well to the varying resource and financial capacity of individual municipalities. This need for scalability is necessary because the CGICTPF does not really cater for this aspect. This is due to the fact that it is aimed at all spheres of government, including provincial and national government, where resources and financial capacity resides in abundance. This is in direct contrast to local government, where a lot of municipalities are small, low-capacity municipalities.

Financial and resource constraints are not the only challenges that the CGICTPF fails to address. Administrative resources are also a concern as there is a huge ICT skills shortage in local government, with a lot of municipalities having under-qualified professionals with watered-down skills (SALGA, 2012). Thus, the complexity of the CGICTPF is unattainable in the operating environment of local government that is laden with constraints.

3.3.2 The South African Local Government Association

In an attempt to address the complexity of the CGICTPF, the SALGA, drafted a municipalised version of the CGICTPF that was allegedly translated into a more municipal-friendly context and a more attainable scope. This document is called, "A Municipal Guide/Roadmap to Successful ICT Governance" (SALGA, 2012).

Within this document, SALGA discusses the governance of ICT, and related issues, with substantially more detail in comparison to the CGICTPF. Furthermore, this municipalised approach to the governance of ICT is thoroughly contextualised to be applicable in the local government landscape. Thus, the unique challenges that accompany the local government landscape receives a lot of consideration and are a constant theme throughout (SALGA, 2012).

Again, similar to the CGICTPF, this document is oriented towards the governance of ICT and not information security management exclusively. It is necessary to note, however, that in terms of information security practices; this SALGA document does devote slightly more attention to information security practices (SALGA, 2012). However, similar to the CGICTPF, this municipalised version contains a lot of directives and requirements in terms of 'WHAT' must be done and little guidance on 'HOW' to do it.

Therefore, it can be argued that even this municipalised guide to the governance of ICT by SALGA, does not address the complexity issue apparent to the CGICTPF. Rather, the SALGA document provides an elaborate discussion on the challenges that local governments face due to their unique landscape and the related challenges. These challenges of financial and resource constraints, along with the lack of adequate skills, call for a more practical approach that is both workable in the face of these challenges and that extends beyond merely 'WHAT' needs to be done; but rather, to also include guidance on 'HOW' it should be done.

Contrary to the expectations of the DPSA and SALGA, the guiding documents they drafted failed to make a noticeable impact on the practices in local government. This was highlighted by the AGSA in the audit reports in the years following the release of these documents. Thus, various entities collaborated to draft an improved municipal version of the CGICTPF.

3.3.3 Municipal Corporate Governance of ICT Policy (MCGICTP)

MCGICTP was drafted in January of 2015. It was drafted with the intention of replacing the CGICTPF, exclusively at a local government level (Department: Western Cape Local Government, 2015b). This was mainly due to the complexity and difficulty that the CGICTPF posed.

This is highlighted in an internal Circular of the Department of Local Government (DLG) of the Western Cape, as it states that; Upon further investigation it became evident that the CGICTPF, referred to municipalities by the DPSA, was too complex for implementation in municipalities as it did not consider the unique operating environments within municipalities (Department: Western Cape Local Government, 2015a). This Circular further states that the Western Cape DLG took the initiative to lead the development of this MCGICTP, in collaboration with SALGA, the DPSA, as well as the Department of Co-Operative Governance and Traditional Affairs (Department: Western Cape Local Government, 2015a).

The Western Cape DLG took the lead in this initiative, however, the development process included consultations with all of the municipalities in the province (Department: Western Cape Local Government, 2015a). Consequently, an agreement has been made with the AGSA that local government will be audited against the deliverables and timelines of the newly developed MCGICTP and no longer the ‘too complex’ CGICTPF (Auditor-General of South Africa, 2015).

In terms of content, however, the MCGICTP seems to be very similar to the original CGICTPF that it replaced, with the exception of minor contextual adaptations. These contextual changes are largely related to terminology, as there is an effort to make it more applicable to local government. The most significant changes with regard to terminology are the titles of individuals to whom roles and responsibilities are assigned (Department: Western Cape Local Government, 2015b).

However, apart from these contextual changes that make the MCGICTP apparently more applicable in the local government landscape, not very much has changed. This is evident as the MCGICTP also follows a three-phased implementation approach, almost identical to that of the CGICTPF (Department: Western Cape Local Government, 2015b). The deliverables within this three-phased approach of the MCGICTP is depicted in Table 3.3, along with its deadlines (Department: Western Cape Local Government, 2015b).

Table 3.3: MCGICTP Deliverables and Deadlines

PHASE	Phase Deadline:	Deliverable Description:
Phase 1	June 2017	Approved and implemented Governance of ICT Charter
		Governance champion designated
		ICT Manager or Chief Information Officer appointed
		Approved and implemented Risk Management Policy
		Approved and implemented ICT Management Framework
		Approved ICT Security Controls Policy
		Approved ICT Continuity Policy
		Approved ICT Disaster Recovery Plan
		Approved Data Backup and Recovery Policy
		Approved ICT Service Level Agreement Management Policy
		Approved User Access Management Policy
		Approved ICT Operating System Security Controls Policy
		Approved and implemented Internal Audit Plan
		Approved and implemented Portfolio Management Framework
Phase 2	June 2019	Approved ICT Migration Plan
		Approved Enterprise Architecture
		Approved ICT Procurement Strategy
		Approved ICT Performance Indicators
Phase 3	June 2019 onwards	Continuous improvement of Corporate Governance of and Governance of ICT

From Table 3.3, it is clear that the MCGICTP phases set deadlines provide local government with more leniency than that of the CGICTPF. However, apart from the terminology changes and the more lenient deadlines, the MCGICTP is very similar to the CGICTPF. Coincidentally, this only makes it seem like the stakeholders within local government are trying to buy more time for themselves to reach the very same deliverables that were mandated by the CGICTPF.

From the perspective of information security management, the MCG-

ICTP dictates a few more policies with an information security-based theme, to be implemented as part of phase 1 (Department: Western Cape Local Government, 2015b). However, the concern remains with the new municipalised version, where no additional guidance is provided as to the content that these policies must contain.

Furthermore, due to the overwhelming similarity between the two documents, it is fair to argue that the same challenges remain. This argument is bolstered by the fact that the new MCGICTP, in a similar fashion to its predecessor, provides deliverables that are items on a ‘checklist’. Thus, it can be argued that the MCGICTP also dictates ’WHAT’ needs to be done, with insufficient guidance on ’HOW’ to do it.

3.3.4 Challenges that Local Governments Face with the Implementation

Although the MCGICTP claims that it is adapted to address the unique challenges of the local government landscape, it provides almost the exact same requirements, with a slightly more lenient timeline, for all municipalities regardless of capacity. These capacity constraints that apply to both finances and skilled personnel, cannot be overcome with a ‘one size fits all’-type approach. Therefore, contributions towards the local government in its quest to improve its governance of ICT, including information security practices as a part thereof, needs to scale well to the various categories of municipalities, with regard to these capacity constraints.

Thus, without the proper skilled personnel, or the financial capacity to acquire such, the MCGICTP will leave low capacity-municipalities stranded without much-needed additional guidance on HOW to achieve the desired deliverables. For this reason, the MCGICTP cannot readily be implemented in all municipalities as is. Furthermore, although the fairly static approach of the MCGICTP might reap benefits in the short term, it is hard to believe that such an implementation that is untailored to the needs of individual municipalities, will be sustainable.

Consequently, the lack of guidance on ‘HOW’ to implement the deliverables and their intricacies, dictated by the MCGICTP, still hints towards it being ‘too complex’, just like the CGICTPF. Thus, low capacity-municipalities with poor resources will struggle with implementing such a vast undertaking, specifically if located in rural areas.

Lastly, from an information security management perspective, a contribution to local government and its information security practices has to incorporate a structured approach that coincides with international standards and related best practices, to add value in this regard. Information security management issues should ideally be addressed with dedicated focus and a clear-cut strategy, and not as an accessory that falls by the wayside; which will most likely be the case as the MCGICTP-implementation continues to unfold.

All the above-mentioned concerns make it clear that criteria to address the capacity issues as well as the lack of adequate skills, need to be defined to address the 'HOW' aspect of sound information security management implementation.

3.4 Criteria for Sound Information Security Management in Local Government

The challenges related to financial constraints and a shortage of skilled personnel that local government face, are in many ways similar to that of Small, Medium and Micro-sized Enterprises (SMMEs). However, in comparison to normal SMMEs, these challenges are intensified in local government, due to the urgency by which improvement is expected and the public nature of the audits of the AGSA. Thus, in order to overcome these challenges, any contribution towards assisting local government, needs to be structured in a way that caters for this unique operating environment. To address this, criteria will be argued that should enable the framework of this research study, to significantly assist local government, in spite of their many challenges.

The first of these criteria aims to consider and address the varying resource capacity of individual municipalities. Thus, the framework for local government should be SCALABLE, to cater for the full scope of municipalities, in terms of financial and resource capacity. SALGA states that, "Municipalities operate in a very isolated non-uniform manner" (SALGA, 2012); which further motivates the need for a contribution that scales really well, due to the non-uniformity across local government. The scalability of the contribution should enable municipalities to implement information security management in spite of financial and resource constraints.

Secondly, the framework should meet the criterion of being USABLE and should enable municipalities to readily implement it, with the need for additional guidance being minimal. The criterion of USABLE, in this context, refers to the, "Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." (ISO/IEC 9241:11, 1998). In the context of this research, however, the term product is irrelevant and refers, rather, to the framework which forms the research contribution. The specified users, refer to local government and all its relevant information users; while the specified goals, refer to the quest for local government to implement effective and sustainable information security management practices.

Thirdly, the contribution should be SIMPLISTIC, in order to further address the shortage of skilled personnel. The simplicity of the framework should aim to empower employees that are not highly skilled, to also be able to implement sound information security management. Regarding the aforementioned, SALGA breaks the harsh reality that, "Staff is made up of under-qualified professionals with watered-down skills that are not geared for real-life ICT crises and challenges" (SALGA, 2012). In addition to having a skills shortage, financial constraints often leave low capacity municipalities even more vulnerable because they cannot afford to involve external consultants.

Finally, the framework should be HOLISTIC so that it addresses the topic of information security and the management thereof comprehensively. In this quest to ensure that information security practices are covered comprehensively, established best practices and international standards should be consulted and drawn from, to form the basis of the framework. This should further enable local government to achieve effective and sustainable information security management, by addressing collectively, the financial constraints and the shortage of skilled personnel within local government.

3.5 Conclusion

This chapter set out to discuss information security management from the perspective of local government, focusing firstly on the current status. After which, the chapter continued on to discuss the initiatives within the local government sphere and the challenges it faces in this regard. Finally, criteria were argued towards addressing these local government challenges in its quest towards implementing effective and sustainable information security management.

Financial constraints and the lack of skilled personnel were pointed out as two of the key challenges within the operating environment of local government, which have to be overcome in order to move forward. These challenges, however, are heightened by the fact that municipalities operate in an independent and non-uniform manner. Furthermore, the alarming fact that 30% of municipalities are poor-resourced and low capacity in nature, further riddles the landscape of local government with difficulty.

Thus, the envisaged framework is based on the argued criteria in section 4.4, as these ensure that the challenges experienced in low capacity municipalities are addressed satisfactorily. The above-mentioned criteria require that the framework should be SCALABLE, USABLE, SIMPLISTIC and HOLISTIC. The contribution of this research study should, therefore, substantially improve and assist information security management within local government; given that these criteria are incorporated into the framework.

The following chapter will discuss the research approach and design, along with the processes and methods utilised in the development and refinement of the contribution, as well as in its eventual validation.

Chapter 4

Research Approach

This chapter aims to describe the research approach that was followed throughout this research project. Firstly, the research paradigm is described. Secondly, a description of the research process, within the specified paradigm, follows. Thirdly, this chapter will contextualise the research process to this research study; before discussing the methods utilised in conducting this research and finally, there is a conclusion to the chapter.

4.1 Introduction

From the previous chapters, it is clear that the problem addressed by this research study is the lack of effective information security management within local government. However, in order to address this problem, a clearly defined research approach has to be followed to enable the research objectives to be met with sound academic rigour.

Thus, the aim of this chapter is to comprehensively describe the research approach followed in this study. This will be done by firstly, discussing the research paradigm that this research was guided by. Secondly, the research process within that paradigm will be described and thirdly, the contextualisation of that process as it applies to the specific details of this study will be highlighted. Finally, the methods used with the research process and its various phases, will be discussed.

4.2 Research Paradigm

The research paradigm that this study adheres to is design-oriented Information Systems (IS) research, as described by Österle et al. (2010). The design-oriented nature of this research paradigm, as the name implies, aims to design and develop artefacts, namely; constructs, models and methods, amongst others, in order to address the identified industry related problem (Österle et al., 2010). Furthermore, according to Österle et al. (2010), concrete manifestations of such artefacts can be axioms, guidelines, frameworks, norms, patents and business models, amongst others.

This same paper states that research within this paradigm strives to be rigorous, yet relevant (Österle et al., 2010). The relevance of research results is vital to this paradigm, as further elaborated in the aforementioned paper; "The most prominent objective of design-oriented IS research is to produce practically beneficial, business relevant results" (Österle et al., 2010). Thus, research within this paradigm aims to address either a tangible problem or improve on an existing real-world implementation (Österle et al., 2010).

Additionally, research within this paradigm is conducted by targeting, and collaborating with, the stakeholders that provide resources for the resolution of the problem (Österle et al., 2010). These stakeholders can commonly include various economic players, such as companies, managers and employees, public administration, the political system, along with various groups of society (Österle et al., 2010). In addition, these stakeholders that are to benefit from the research study demand that design-oriented IS research yields an artefact, which contributes to and benefits the identified problem area (Österle et al., 2010).

Furthermore, Österle et al. (2010), state that their paper aims to provide rules for scientific rigour and improved guidance for researchers when working within this paradigm. Thus, design-oriented IS research prescribes the following principles that must be adhered to, in order to conform to the parameters of this paradigm (Österle et al., 2010).

Consequently, all four of the principles in Table 4.1 have to be adhered to, for research aims to be in adherence of this paradigm. However, as long as the principles in Table 4.1 are adhered to, design-oriented IS research allows the researcher to enjoy substantial academic freedom in the use of research

Table 4.1: Principles for Design-Oriented IS Research

Research Principle	**Description**
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 comprehensible manner and must allow for its validation
Benefit	Each artefact must yield benefit either immediately or in the future for the respective stakeholders

methods, publication of research results and stakeholder satisfaction (Österle et al., 2010).

Although this paradigm allows for academic freedom, there is a typical research process that is recommended for use within this paradigm (Österle et al., 2010), which will be discussed in the following section.

4.3 Research Process

The design-oriented IS research paradigm prescribes the following four-phased process as common practice. The four phases of design-oriented IS research are: *Analysis, Design, Evaluation* and *Diffusion,* respectively, as depicted in Figure 4.1 (Österle et al., 2010).

This process is iterative in nature, as depicted in Figure 4.1, with as many cycles as necessary to refine the artefact to both, the researchers and the practitioners satisfaction (Österle et al., 2010).

However, this process does not provide sufficient guidance as to the tech-

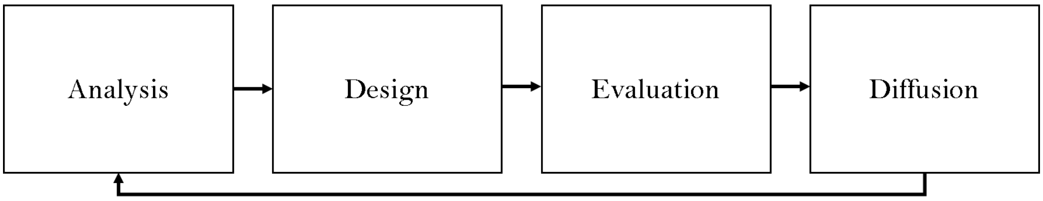


Figure 4.1: Design-Oriented IS Research Process

nical detail that needs to be addressed throughout these phases. To address this, an alternate research process with similar goals was used to supplement the process of design-oriented IS research. The above argument will not impede the research results, as the design-oriented IS research paradigm provides the researcher reasonable academic freedom, as long as the research principles presented in section 3.2 are adhered to (Österle et al., 2010).

The paradigm of Design-Based Research (DBR) was chosen as the alternative research approach which was used in combination with that of design-oriented IS research. This DBR paradigm stems from the field of educational technology and learning sciences (Reeves, 2006). The DBR goals are very similar to the goals of design-oriented IS research, as they also advocate the design of artefacts that contribute to real problems in practice, in collaboration with the practitioners or stakeholders (Reeves, 2006). The above mentioned similarities and the extensive guidance and detail within the phases of DBR served as the key persuading factor to use the DBR process. Furthermore, the DBR approach is also an iterative process, with freedom for the repetition of each of the four phases until the artefact is satisfactory, as depicted in Figure 4.2 (Reeves, 2006).

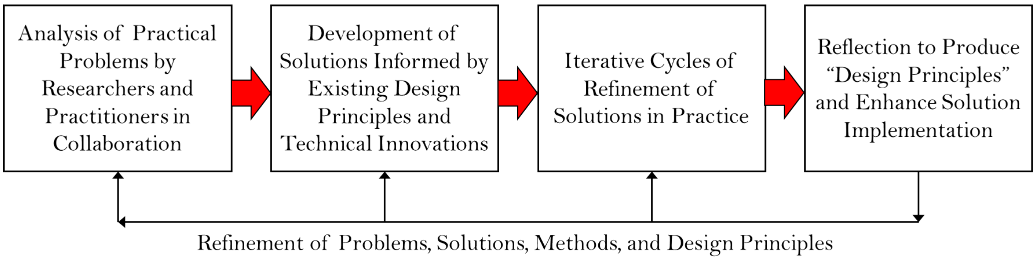

Analysis of Practical Problems by Researchers and Practitioners in Collaboration
Development of Solutions Informed by Existing Design Principles and Technical Innovations
Iterative Cycles of Refinement of Solutions in Practice
Reflection to Produce "Design Principles" and Enhance Solution Implementation
Refinement of Problems, Solutions, Methods, and Design Principles

Figure 4.2: Design Research in Educational Technology Research

As mentioned before, the process of the DBR paradigm was used as it provides much more detailed guidance in conducting each phase (Herrington, McKenney, Reeves, & Oliver, 2007). This detailed guidance provides the researcher with various elements that should be addressed in each phase (Herrington et al., 2007). These elements within each phase of the DBR paradigm are depicted in Table 4.2 (Herrington et al., 2007).

These elements of the DBR process will supplement the design-oriented IS research paradigm used in this study. Consequently, the two will be in-

Table 4.2: Design-based Research: Elements in Phases

Phase	**Element**
Phase of design-based research	*The elements that need to be completed*
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem
	Consultation with researchers and stakeholders
	Research objectives
	Literature review
PHASE 2: Development of solutions informed by existing design criteria and technological innovations	Theoretical Foundation
	Development of criteria to guide the design of the intervention
	Description of proposed intervention
PHASE 3: Iterative cycles of testing and refinement of solutions in practice	**First iteration**
	Participants
	Data collection
	Data analysis
	Second and further iterations
	Participants
	Data collection
	Data analysis
PHASE 4: Reflection on criteria of produced artefact; and enhance solution implementation	Design Criteria
	Designed artefact(s)
	Professional development

* Note: Adapted from Herrington et al. (2007)

tegrated into a tailor-made integrated research approach. Furthermore, by integrating these two research processes, this research study will be conducted within the design-oriented IS research paradigm, following the detailed research process guidelines from DBR. From the perspective of the DBR process, this is also acceptable, as this integration aligns with Herrington et al. (2007), as they encourage researchers to adapt these elements to suit their own purposes.

The four phases from design-oriented IS research and the, near similar, phases from DBR can be integrated along with the research elements from DBR. This can lead to the integrated research process utilised in this research project. Also, the elements from the process of DBR are included in this integrated research process. All of this is depicted in Figure 4.3.

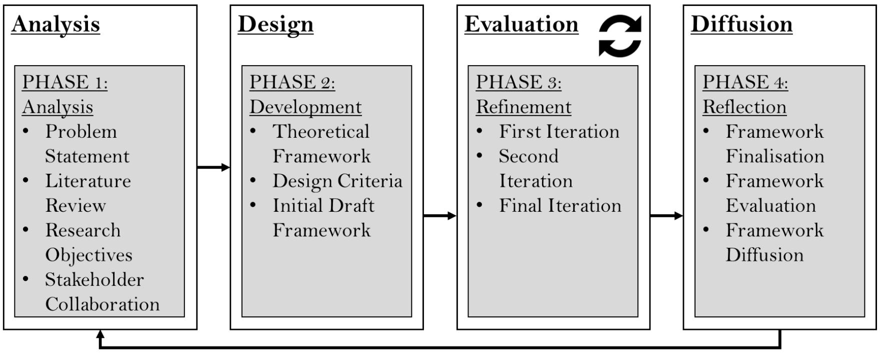


Figure 4.3: Integrated Research Process

From Figure 4.3 it is clear that the first phase of *Analysis* is where the research is planned, as the problem is defined. This is done by consulting relevant literature and by collaborating with necessary stakeholders. After which, objectives are set to address the problem. Furthermore, in the second phase of *Design*, the initial draft of the framework is developed, which forms the first draft of the eventual contribution of this research study, along with the criteria to guide its development. After this initial draft of the framework is developed, it undergoes various cycles of refinement, in the third phase of *Evaluation*. In this third phase, the refinement cycles are repeated until both the researchers and the stakeholders are satisfied with the resulting framework. Finally, in phase four which is *Diffusion*, the framework is documented and validated.

These guiding objectives or deliverables within every phase are essentially the elements proposed within the DBR research process. Thus, Figure 4.3 illustrates the integrated research process and its elements that will be used for this study. The elements associated with the various phases, as depicted in Table 4.2, will be contextualised in the following section to be applicable to the unique parameters of this research study.

4.4 Research Process in Context

The previous section discussed the tailor-made integrated research process of this study. This section will discuss each of the phases of this process individually. Furthermore, these phases will be placed within the context of this study.

This tailor-made integrated research process will now be further contextualised in detailed tables, as it applies to this research study.

4.4.1 Phase 1: Analysis

Table 4.3 depicts the context of the elements of the Analysis phase within this study.

Table 4.3: Design-based Research Phase 1

PHASE	**ELEMENT**	**POSITION**
Phase of design-based research	*The topics/elements that need to be described*	*Position in research project*
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem Consultation with researchers and stakeholders	An initial problem was identified by consulting with stakeholders in local government
	Literature review	A literature review was conducted to further refine the understanding of the problem
	Research objectives	In order to address the stated problem, relevant objectives were defined

As seen in Table 4.3, the problem was initially identified by consulting with various representatives from local government. Relevant literature was then studied to both verify and refine the problem, after which, objectives were defined for this study to guide the researcher in addressing the problem.

Consequently, due to the design-oriented nature of this study, the objectives aim to guide the development of an artefact, in the form of a framework, which forms the research contribution.

4.4.2 Phase 2: Development

This phase is where the initial design of the draft framework is done, as illustrated in Table 4.4.

Table 4.4: Design-based Research Phase 2

PHASE	**ELEMENT**	**POSITION**
Phase of design-based research	*The topics/elements that need to be described*	*Position in a research project*
PHASE 2: Development of solutions informed by existing core aspects and technological innovations	Theoretical foundation	Study international standards and best practices (theoretical framework) in contrast to current status of ISM in local government to extract criteria to guide design
	Development of criteria to guide the design of the intervention / framework	
	Description of proposed framework	Develop initial draft framework from theoretical foundation, incorporating the criteria

In this study, the

first two elements of the Development phase, theoretical framework and the development of criteria, were addressed together as they complement each other and serve the same end-goal, as depicted in Table 4.4. Essentially, the theoretical framework for this study is largely based on the relevant international standards and academic publications, upon which the framework is based. The best practice components of sound information security management are compared to the current status thereof within local government.Consequently, this comparison then highlights the gaps in the current implementation of information security management practices within local government. These gaps are addressed by developing criteria that are incorporated into the design of the framework. Finally, taking all the above into consideration, the initial draft framework is developed.

4.4.3 Phase 3: Refinement

Within the Refinement phase, this initial draft of the framework is evaluated and refined in an iterative manner (See Table 4.5). These iterations of refinement continue until both the researcher and the stakeholder are satisfied with the framework.

Table 4.5: Design-based Research Phase 3

PHASE	**ELEMENT**	**POSITION**
Phase of design-based research	*The topics/elements that need to be described*	*Position in a research project*
PHASE 3: Iterative cycles of testing and refinement of solutions in practice	**First iteration** (Implementation of intervention)	Iteration commences with initial draft framework
	Stakeholders	Representatives from local government
	Data collection (Mixed Research Methods)	Framework is tested for acceptance
	Data analysis	Data interpretation and critical analysis thereof
	Implementation of intervention	Second draft of artefact (framework) towards good CGICT in local government
	Second and further iterations (same elements as first iteration)	Second iteration commences with adapting the initial draft framework based on engagement with stakeholders. Further iterations build on the output from the previous iteration.

From Table 4.5, it is clear that within the first iteration, the initial draft of the framework is presented to representatives from local government, as the stakeholders. Upon engaging with the stakeholders, with the aim of refining the framework, the data collected is analysed so that the framework can be adapted and improved accordingly. This complete refinement iteration process is repeated as many times as is necessary.

4.4.4 Phase 4: Reflection

Finally, the Diffusion phase is where the framework is finalised, distributed to the stakeholders as widely as possible and the framework is documented and published. This fourth and final phase is depicted in Table 4.6.

Table 4.6: Design-based Research Phase 4

PHASE	**ELEMENT**	**POSITION**
Phase of design-based research	*The topics/elements that need to be described*	*Position in a research project*
PHASE 4: Reflection to produce "Design Criteria" and enhance solution implementation	Design Criteria	Ensure that the framework adheres to the following criteria (apparent to phase 2 - Design): • Usable • Simplistic • Scalable • Holistic
	Designed artefact (framework)	Finalisation of framework for ISM in local government
	Professional development	Make available (Diffuse) to local government as far as possible and publish the framework

Within this phase, the design criteria are ensured through some form of validation exercise. After which, the framework is finalised and made available to local government as far as possible and the framework is published.

Thus, the detailed guidance gained from the elements of the DBR research process enables the researcher to best address the problem at hand. However, the design-oriented IS research paradigm provides the researcher with reasonable freedom as to which methods to use. Therefore, the following section will discuss the various research methods used in this study.

4.5 Research Methods

As mentioned before, this research study aims to develop an artefact, in the form of a framework, to address a practical problem faced by business, or rather local government in this case. In order to achieve this, various research methods were used. The methods were chosen as they are best suited to the unique problem area and design of this research study.

Initially, literature review was used to identify the problem that this study aims to address. The problem was then verified and refined further by making use of semi-structured interviews, which were conducted with various stakeholders within local government. Furthermore, the literature review in this research study extended beyond merely identifying the problem. It also included studying relevant international standards, academic publications and government policies amongst others, to identify the elements and/or components of sound information security management. These components are essentially what the framework is based on.

Consequently, once the basis of the framework was established from literature, the initial draft of the framework was formulated. Part of this initial draft of the framework included elements of modelling, in order to give a visual representation of the intricacies of the framework. The framework was then presented to stakeholders within local government via the medium of focus group discussions. These focus group discussions served the purpose of engaging with local government with the intent of refining the framework. Several iterations of these focus group discussions followed until both the researchers and the stakeholders found the framework to be satisfactory.

Once the framework was finalised after the final iteration of refinement, prototyping was used to develop a spreadsheet-based tool in support of the framework. This spreadsheet-based tool was presented to representatives of local government in order to validate the framework against the design criteria that it set out to meet (see section 3.4). In order to complete this validation (see Chapter 6), questionnaires were used to obtain the necessary feedback and acknowledgement from the local government representatives.

All of the research methods that were used in this study are defined in Table 4.7, as well as placing them within their corresponding phases of the research process.

Table 4.7: Research Methods & Definitions

Research Method	**Phase in Process**	**Definition**
Literature Review	Phase 1 and 2	An iterative process of obtaining information sources relevant to one's study (Olivier, 2009)
Semi-structured Interview	Phase 1	A verbal exchange where the interviewer attempts to elicit information from another person, or group of people, by asking questions. Although there is a set of predetermined questions, this interview is conversational in nature and allows participants to explore the topic and related issues as they see fit (Longhurst, 2003)
Modelling	Phase 2 and 3	A model captures the essential aspects of a system or process, while it ignores the non-essential aspects and can serve as a blueprint for new systems or processes (Olivier, 2009)
Focus Group	Phase 3	Involves a group of people who meet in an informal setting to talk about a topic set by the researcher and allows for subject to explored from as many perspectives, or viewpoints, as they please (Longhurst, 2003)
Prototype	Phase 3	A representation of a design idea, regardless of medium (Houde & Hill, 1997)
Questionnaire	Phase 4	An instrument consisting of a series of questions and/or attitude opinion statements designed to elicit responses which can be converted into measures of the variable under investigations (Franklin & Osborne, 1971)

4.6 Conclusion

This chapter defined the research approach of this study. It should be clear that this study is placed within the design-oriented IS research paradigm. Within this paradigm, researchers aim to develop rigorous, yet relevant artefacts, in collaboration with stakeholders to address a problem. The stakeholders expect a specific benefit to yield from their collaboration with the researchers.

The design-oriented IS research paradigm allows the researcher reasonable academic freedom, as long as the four principles of this paradigm are adhered to. These four principles are: Abstraction, Originality, Justification and Benefit. The research process of this paradigm consists of four phases and is iterative in nature. However, for the purpose of this study, the research process of design-oriented IS research was deemed to provide insufficient guidance to the researcher. Thus, this research process was supplemented by integrating the research process of DBR paradigm, from the field of educational technology.

This unique integrated research process contains specific elements that constitute the four phases of this research process. Furthermore, various research methods were used to complete these four phases satisfactorily. The following chapter will discuss the framework, which is the artefact that stems from this research study.

Chapter 5

A Framework for Information Security Management in Local Government

This chapter aims to describe the research artefact, in the form of a framework. Firstly, the process leading up to the development of initial draft of the framework is discussed. Secondly, the details of the refinement iterations that were conducted are explained. Finally, the resultant framework is discussed in this chapter, after the completion of all refinement cycles; before concluding this chapter.

5.1 Introduction

In the previous chapter, the unique integrated research process that was utilised in order to address the problem at hand was described. This problem was addressed by following the afore mentioned integrated research process, which resulted in the development of an artefact. This chapter is, therefore, devoted to describing the resulting framework of this research study. This framework for information security management will be termed FISM and will be discussed in two parts; Part A and Part B.

Part A will describe how the unique integrated research process was used in order to develop the artefact (FISM). Within Part A, the first three phases of the unique integrated research process will be discussed individually, highlighting how the phases contributed towards the development of this framework. Following that, Part B will discuss the details of the FISM and all of its components.

5.2 Part A: Developing FISM

Within this section, the development of the framework is discussed in detail. This development of the framework is achieved throughout the first three phases of the integrated research process that was highlighted in Chapter 4. The position of this section within the integrated research process is depicted in Figure 5.1.

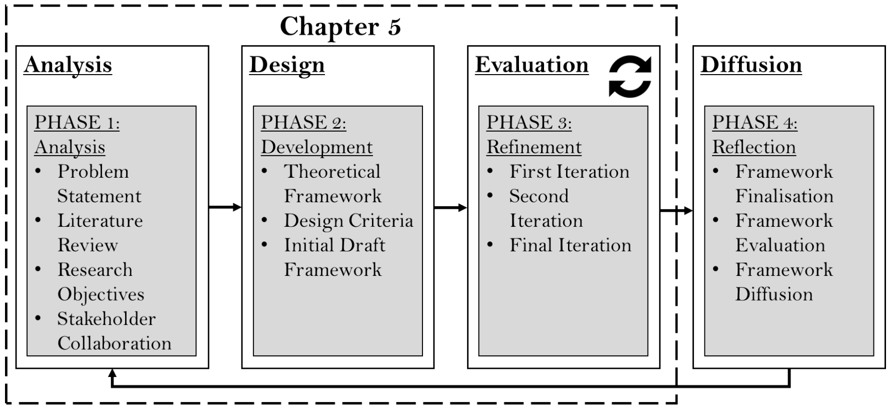


Figure 5.1: Integrated Research Process Development of Framework

The following subsections will discuss these three phases individually and discuss how their respective elements contributed to the development of the framework. It is clear from the previous chapter what the elements entail. However, the focus will fall on how those elements were applied in this study within the subsections that follow.

5.2.1 Phase One: Analysis

The first phase, Analysis, and its elements are the focus in this subsection. The elements of this phase are listed in Table 5.1. From this, it is clear that this phase is comprised of a literature review, consultations with researchers and stakeholders, the problem statement and research objectives, respectively. However, it is important to note that Table 5.1 does not necessarily list the elements in chronological order. Rather, the chronological order of how the elements transpired in this study is provided by the remainder of this subsection.

Table 5.1: Elements of Phase 1: Position within Research Study

PHASE	**ELEMENT**
Phase of design-based research	*The topics/elements that need to be described*
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem
	Consultation with researchers and stakeholders
	Literature review
	Research objectives

Initially, the problem was identified that this research aims to address by studying relevant literature through a literature review. This literature review highlighted the concerning nature of information security management within local government. The primary source that highlighted this problem was the AGSA Audit Reports on the status of controls in local government. However, the voice of concern raised by the AGSA was not a solitary one. Local government themselves drafted various policy documents to remedy the problem (See Chapter 3). Thus, it is clear that local government has acknowledged this problem and are attempting to change this.

Consequently, two stakeholder meetings were arranged in order to better understand the problem and the possible causes thereof. These two stakeholder meetings were held on 30 and 31 March of 2015, respectively. Both meetings were facilitated by making use of semi-structured interviews.

The first meeting was held with a representative of the Department of Co-Operative Governance in the Western Cape. The problem was undoubtedly confirmed at this meeting, as the representative had extensive insight into the status of the ICT function in all municipalities within the Western Cape. This meeting particularly highlighted how the ICT function, as a whole, operates within local government. Additionally, the newly drafted governing policy for ICT within local government, the MCGICTP, was introduced for the first time to the researcher. The understanding gained from this interaction provided a good foundation for the second stakeholder meeting of the following day.

The second meeting was held with the ICT managers and several risks, internal audit and technology officials of a district municipality in the Western Cape. This included the ICT managers of all the subordinate local municipalities that form part of the district. This specific district municipality was selected as a contributing stakeholder in this study due to a longstanding clean audit of its ICT function by the AGSA. Within this meeting, it was highlighted that a lack of skills and resources are a big hindrance to information security management in local government. This painted a clearer picture of why the problem exists and provided a better understanding with which to address the problem. This district municipality agreed to be the primary stakeholder throughout the iterative refinement process of phase 3 of this study.

Finally, the research objectives of this study were formulated based on the initial problem that was identified, in combination with the better understanding gained from the two respective stakeholder engagements (See Chapter 1). The initial draft of the framework was constructed in order to address the problem at hand. This development of the initial framework will be discussed in the following section.

5.2.2 Phase 2: Development

The previous Analysis phase, drew from literature in order to identify the problem that this research aims to address. Within the Development phase, a literature review was used to establish the theoretical foundation upon which FISM is based. This theoretical foundation is essentially the core components of what information security management practices entail in the modern era (See Chapter 2). Establishing the theoretical foundation of FISM is the first element listed in Table 5.2.

The second element in Table 5.2 is design criteria for the development of FISM. The design criteria mentioned here is the same criteria argued towards in Chapter 3. These criteria are; SCALABLE, SIMPLISTIC, HOLISTIC and USABLE, respectively.

These criteria are built into FISM, in addition to the theoretical foundation of core components to information security management. Thus, the initial draft of FISM was developed, while taking both of these elements into

Table 5.2: Elements of Phase 2: Position within Research Study

PHASE	ELEMENT
Phase of design-based research	*The topics/elements that need to be described*
PHASE 2: Development of solutions informed by existing design criteria and technological innovations	Theoretical foundation
	Development of criteria to guide the design of the intervention / framework
	Description of proposed framework

consideration. This initial framework is depicted in Figure 5.2.

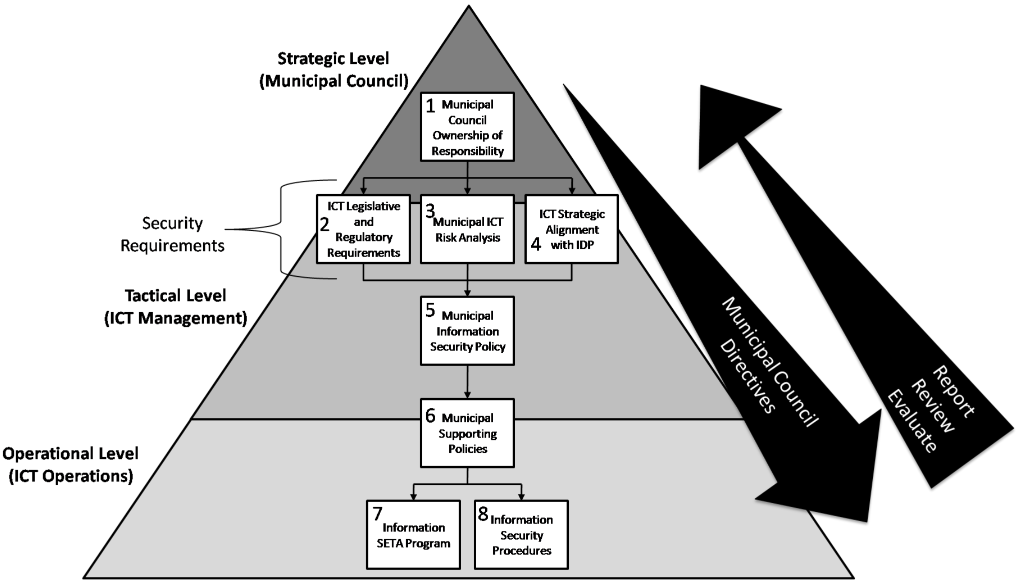

Strategic Level
(Municipal Council)
1 Municipal Council Ownership of Responsibility
Security Requirements
2 ICT Legislative and Regulatory Requirements
3 Municipal ICT Risk Analysis
4 ICT Strategic Alignment with IDP
Tactical Level
(ICT Management)
5 Municipal Information Security Policy
Operational Level
(ICT Operations)
6 Municipal Supporting Policies
7 Information SETA Program
8 Information Security Procedures
Municipal Council Directives
Report Review Evaluate

Figure 5.2: Initial Draft Framework

5.2.3 Phase 3: Refinement

The initial draft of FISM, illustrated in Figure 5.2, was essentially the starting point of this framework. This initial draft framework was the subject of the first cycle of refinement apparent to the third phase of Refinement. As depicted in Table 5.3, the first iteration of refinement involved engaging with relevant stakeholders and collecting data from these engagements. The data collected was analysed and based on that, an intervention or changes followed accordingly. The second and all further iterations consist of the exact same elements and structure.

Table 5.3: Elements of Phase 3: Position within Research Study

PHASE	ELEMENT
Phase of design-based research	*The topics/elements that need to be described*
PHASE 3: Iterative cycles of testing and **refinement** of solutions in practice	**First iteration** (Implementation of intervention)
	Stakeholders
	Data collection (Mixed Research Methods)
	Data analysis
	Implementation of intervention
	Second and further iterations (same elements as first iteration)

Regarding the first iteration, however, the details of how it was completed are described in the following subsection.

Refinement Iteration 1

The first refinement iteration of FISM was conducted via a meeting with the relevant stakeholders, in the form of a focus group. This focus group meeting took place on 4 June 2015. The stakeholders from local government that participated in the focus group were several representatives of the ICT and risk functions of the district municipality described in the first phase, that of *Analysis*.

The focus group was used as the platform from which the initial draft framework (Figure 5.2) was discussed and analysed. The goal of this discussion was to gain insight into the efficacy and applicability of the framework to the problem by members of the district municipality directly involved in its information security management practices.

Based on the discussions of this focus group, the researcher had to analyse the comments and suggestions made in the focus group. The analysis of these comments and suggestions were then used to adjust, improve and change FISM as necessary. The changes and improvements made to FISM were made by finding a balance between the recommendations of the district municipality representatives and what literature prescribes as common best practice. This was done to ensure that the framework is tailor-made to the requirements of the specific problem, while still providing the framework sound theoretical rigour.

The changes and improvements made after this engagement with the district municipality representatives led to FISM being simplified, as depicted in Figure 5.3. The need for simplicity was stressed by the representatives from the district municipality due to the lack of resources and skills that plague local government at large.

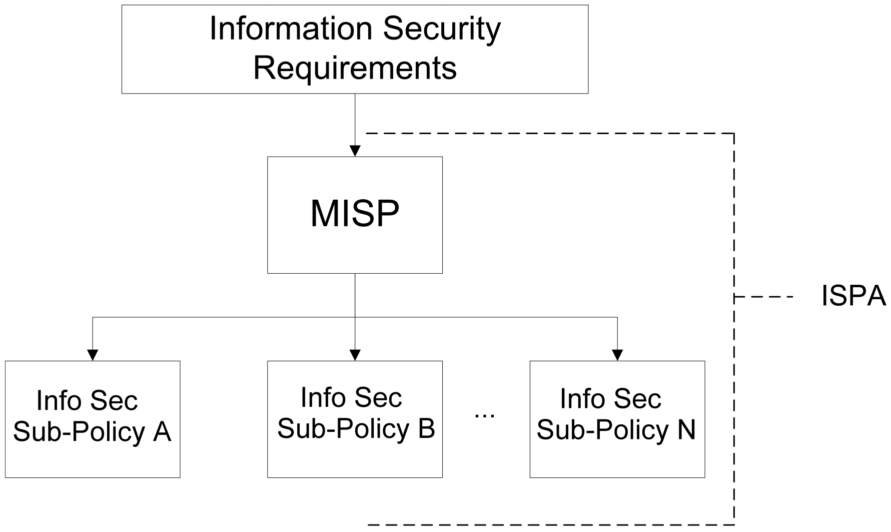


Figure 5.3: Second Draft Framework (Architecture of Framework)

The *architecture* depicted in Figure 5.3, is the second draft of the initial draft framework. This architecture has essentially been limited to merely consist of the Information Security Policy Architecture (ISPA) portion of the initial draft framework. This is due to the fact that the initial draft contained many aspects of security governance and corporate governance, which are beyond the scope of this study. Thus, to focus only on the ISPA as the core *architecture* is more applicable to the information security management challenges that local governments face.

This ISPA that was proposed as the second draft of the framework consists of a high level Municipal Information Security Policy (MISP), with as many security sub-policies as needed. These policies collectively constitute an ISPA and should stem from the unique and specific information security requirements of a municipality. However, this *architecture* depicted in Figure 5.3, merely provides a blueprint of WHAT a municipality should typically implement to address information security management. Therefore, a second iteration was conducted to both improve and supplement this *architecture* further.

Refinement Iteration 2

The focus group meeting during the second refinement iteration was held on 19 August 2015. This focus group meeting again involved the same district municipality representatives and the discussion explored the second draft of FISM, as seen in Figure 5.3. Similar to the first refinement iteration, the purpose of the focus group was to collect sufficient data so that FISM can be improved.

The simplification of the framework, evident in Figure 5.3, was satisfactory according to the representatives who participated in the focus group. However, this second draft of the framework only prescribes '*WHAT*' should be implemented and lacks additional guidance on '*HOW*' to attain it. Thus, the framework was expanded to not only include the '*architecture*' in Figure 5.3, but also the '*Process*' depicted in Figure 5.4.

The process depicted in Figure 5.4, proposed six main steps by which a municipality can generate the proposed ISPA of the *Architecture*, as seen in the first iteration. Step one of the *Process* presents the security categories of ISO/IEC 27002 for consideration in the form of a questionnaire. Upon which during step two, these security categories have to be considered and deemed either applicable to the needs of the specific municipality or not. All security categories that are indeed deemed as applicable are then studied more carefully at step three of the *Process*.

Once the security categories are thoroughly scrutinised and understood, the categories are either selected for implementation or rejected with sufficient justification for its exclusion during step four. For all security categories that are selected for implementation, the security controls of ISO/IEC 27002 within those categories are to be considered (step five). Once all security controls of the selected categories were considered, the controls also have to

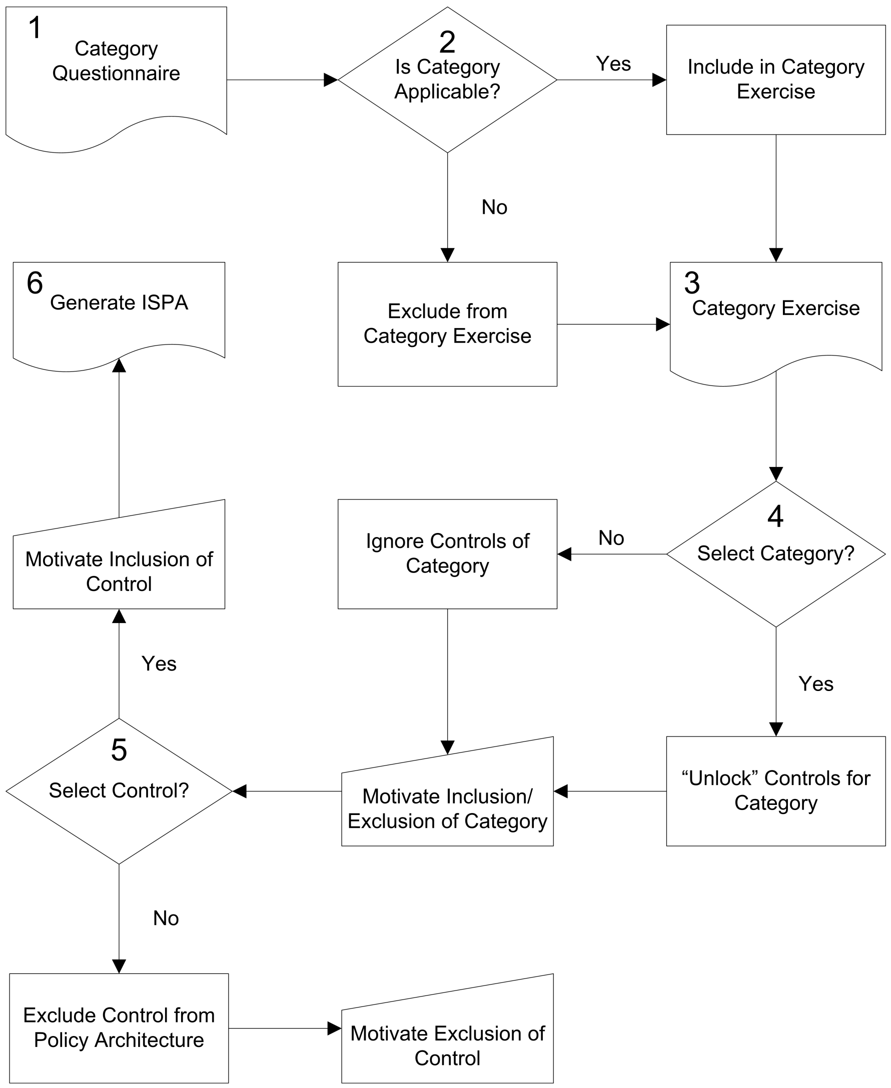

1
Category Questionnaire
2
Is Category Applicable?
Yes
Include in Category Exercise
No
6
Generate ISPA
Exclude from Category Exercise
3
Category Exercise
4
Select Category?
No
Ignore Controls of Category
Motivate Inclusion of Control
Yes
Yes
5
Select Control?
Motivate Inclusion/ Exclusion of Category
"Unlock" Controls for Category
No
Exclude Control from Policy Architecture
Motivate Exclusion of Control

Figure 5.4: Third Draft Framework (Process of Framework)

be either selected for implementation or rejected with sufficient justification for its exclusion.

Finally, at step six of the Process the security categories, along with their underlying controls, that were selected for implementation are translated into applicable policy documents to form an ISPA that is specific to the requirements of the municipality. This ISPA will typically consist of an MISP, supplemented by supporting sub-policies. The security categories should typically be integrated into the MISP, while the controls populate the supporting sub-policies.

Refinement Iteraion 3

The third and final iteration of refinement consisted of a focus group meeting, which took place on 17 November 2015. This focus group meeting included the same group of representatives, within its ICT and risk functions, from the district municipality. This iteration focused on improving the newly drafted component of the framework, the process depicted in Figure 5.4.

The discussion of the focus group session was again analysed with the aim of improving the framework. Consequently, the process component of the framework was adjusted accordingly. However, the architecture component (Figure 5.3) was also discussed briefly and improved accordingly.

Both components, the architecture and the process that supplements it constitute the framework (FISM) as the goal of this research. The finalised framework will be discussed in detail in the following section, including the changes/improvements that stemmed from this final refinement iteration.

5.3 Part B: Finalised FISM

As mentioned before, local government is continually faced with administrative and financial constraints. Therefore, the framework (FISM) of this research study aims to provide local government with a self-help approach that largely negates the aforementioned challenges of limited resources, both financially and in terms of skilled personnel. This research contribution (in the form of FISM) has two components of which the first is architecture, supplemented by a process that illustrates the proposed steps to implement the architecture. Essentially, the combination of both components forms FISM.

This FISM is described in the following sections after the final iterations of refinement. Thus, it is the improved and finalised versions of the architecture and the process and not the same as seen in Figures 5.3 and 5.4.

5.3.1 Architecture for FISM

The architecture proposed in this subsection provides clarity on the '*WHAT*'-factor for municipalities in terms of information security practices that need to be in place to effectively manage its information security. The content and basis of FISM are in line with what international standards and best practices recommend, as described in chapter 2.

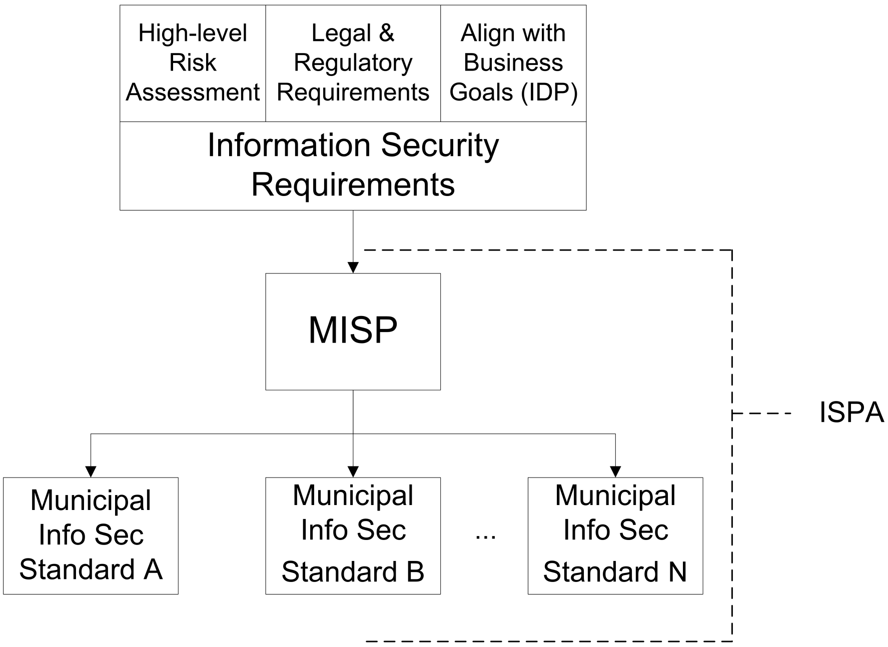

High-level Risk Assessment
Legal & Regulatory Requirements
Align with Business Goals (IDP)
Information Security Requirements
MISP
ISPA
Municipal Info Sec Standard A
Municipal Info Sec Standard B
...
Municipal Info Sec Standard N

Figure 5.5: Architecture for FISM

As depicted in Figure 5.5, the content of the MISP and the supporting Municipal Information Security Standards should be based on the Information Security Requirements of the municipality.

The Information Security Requirements should stem from the results of a high level risk assessment. In addition, it should align information security with strategic business goals, which is typically the Integrated Development Plan (IDP) in the case of municipalities. The Information Security Requirements should also give consideration to the legal and regulatory environment in which the municipality operates.

The MISP serves the role of a high level information security policy that communicates the directives from executive management for information security to all employees. The organisation of information security, as well as the roles and responsibilities for information security, should also be contained in this document. Due to the high level nature of this document, it should be constructed in a non-technical manner without giving guidance for specific processes at an operational level. An example of such an MISP can be seen in Appendix A.

The various Municipal Information Security Standards that stem from the

MISP should provide this more technical and detailed guidance for information security practices. Each of the Municipal Information Security Standards should address specific interrelated issues which can be logically grouped together under one topic, for instance, User Access Management, Internet & Email Usage or Network Security. As Figure 5.5 depicts, the MISP should typically be supplemented with as many security standards (the equivalent of sub-policies) as needed. These security standards, serve to provide more technical detail and guidance on the necessary practices to adhere to the MISP and thus indicate the hierarchical nature of the ISPA.

The ISPA consists of the collection of the MISP and the Municipal Information Security Standards that support it. The ISPA of a municipality should be unique and specific to their Information Security Requirements. This ISPA could easily be generated in an automated manner upon completion of the process, as the process details steps to implement the architecture. This process will be discussed in the following subsection.

5.3.2 Process for FISM

It is important to note that the principles within the ISO/IEC 27000-set of standards form the primary theoretical basis of the framework. Furthermore, as stated previously, the purpose of the process which is discussed in this subsection is to provide municipalities with guidance with which to implement an ISPA through a series of steps. This ISPA serves the purpose of addressing their unique Information Security Requirements as proposed in the architecture. The process essentially provides the detailed steps of '*HOW*' to implement the architecture within a municipality.

This Process for Information FISM has three steps that are depicted in Figures 5.6, 5.7 & 5.8 respectively. The first step in the Process focuses on the categories within ISO/IEC 27002. As depicted in Figure 5.6, the first step of the Process involves a municipality to consider each of the security categories of ISO/IEC 27002 individually, along with the objectives of those categories. Based on the objective of the category, the municipality must select whether or not it applies to them. However, throughout this first step of the Process, the selection of security categories from ISO/IEC 27002 should be based on the unique Information Security Requirements of the municipality. Furthermore, the municipality must Provide Justification for every selection they make, both when they select and decline a category.

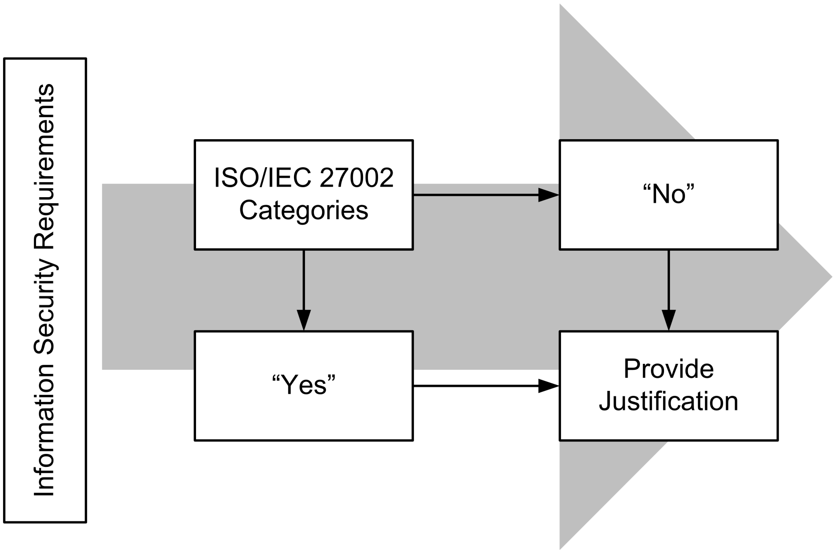


Figure 5.6: Process for FISM - Category Selection (Step 1)

Upon completion of this step of the Process, the categories that are declined by the municipality are ignored and excluded from the remainder of the steps within the Process. However, those categories that are selected by the municipality will be further elaborated upon, as all the controls within those categories should be considered. This is depicted in Figure 5.7.

Again similar to the previous step of the Process, controls should be considered individually, along with the objectives of the controls. The difference, however, is that for every category, there are multiple controls to consider. The selection of every individual control, as depicted in Figure 5.7, should be influenced by the Information Security Requirements. Furthermore, as before, a municipality should Provide Justification for both, the selection and rejection of a control. At the end of this step in the Process, a municipality will have identified a set of controls that is applicable to them, and that they should be able to implement from a resource and capacity perspective.

The final step of the Process, as depicted in Figure 5.8, is completely based on the selection of controls by the municipality. The set of selected controls should be integrated into the ISPA that is applicable to the municipality and its unique operating environment. This is ensured as the selection of these

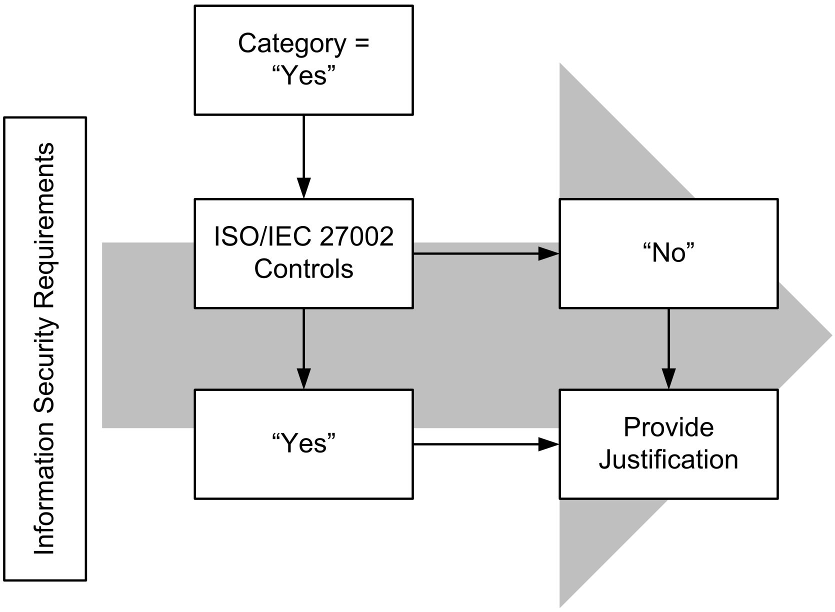


Figure 5.7: Process for FISM - Control Selection (Step 2)

controls was based on the specific Information Security Requirements of the municipality.

The integration of controls into the ISPA can easily be automated by using software, which will simplify the process of implementation. The selected controls should be integrated into and communicated via the ISPA, from the high level MISP right through to the Municipal Information Security Standards, with the relevant amount of details and technicality respectively.

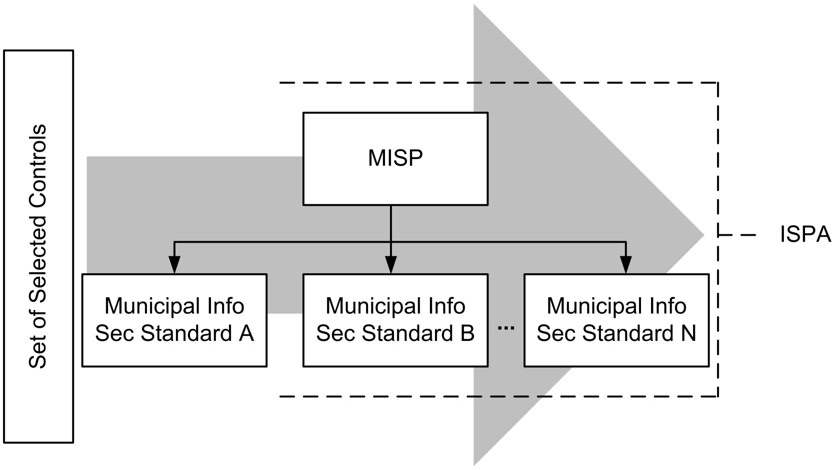

Set of Selected Controls
MISP
ISPA
Municipal Info Sec Standard A
Municipal Info Sec Standard B
...
Municipal Info Sec Standard N

Figure 5.8: Process for FISM - ISPA Generation (Step 3)

5.4 Conclusion

This chapter set out to discuss the framework to emerge from this research study. In doing so, FISM was divided into two parts. Part A described the course of development FISM followed. This included the initial draft of FISM, as well as the consequent refinement thereof. Part B described the finalised framework after the iterations were completed and necessary changes addressed.

FISM consists of two components. The first being, an architecture which describes '*WHAT*' a municipality should typically implement in terms of information security management practices. This is based on the theoretical foundation provided mostly by Chapter 2 of this study.

The second component of FISM is a Process, which describes the necessary steps needed to achieve the implementation of the WHAT-factor. Essentially, this Process provides the guidance on '*HOW*' to implement it. These two components collectively form the contribution of this study.

However, the unique integrated research process this study follows requires the framework to adhere to additional design criteria. This is to ensure that the problem the research aims to address is done with more efficiency by tailoring it to the need of the stakeholder, which in this study is local government. The design criteria as argued before are HOLISTIC, USABLE, SCALABLE and SIMPLISTIC, respectively. The following chapter will describe the validation of FISM against these criteria, which was done by means of a workshop.

Chapter 6

Validation of FISM

This chapter aims to describe the validation of the research artefact against the design criteria. Firstly, the design of the validation process and the data collection are discussed. Secondly, the analysis of the data collected and the results are described. Finally, the findings are discussed before concluding this chapter.

6.1 Introduction

The FISM framework, as the premier contribution of this research study, was described in the previous chapter, which is essentially the research contribution. In accordance with the unique integrated research process that this study follows, FISM should satisfy specific design criteria. These design criteria were highlighted in Chapter 3 and aim to address the challenges that are specific to local government and its implementation of information security management.

This enables the researcher to provide individual municipalities with the means to implement information security management, in a tailor-made manner to fit its specific needs. The benefit of adhering to these design criteria, however, extends beyond the interest of local government as the stakeholder. The additional benefit is yielded to the interest of the researcher in adhering to these design criteria to provide additional scientific rigour to the artefact.

These design criteria, as argued in Chapter 3, require FISM to be SIMPLISTIC, USABLE, SCALABLE and HOLISTIC. This chapter describes the validation exercise of FISM's capacity to adhere to these criteria and the findings that stemmed from the validation exercise. The validation exercise was completed by facilitating a workshop with several local government officials to demonstrate a proof of concept of FISM. The structure and design of the workshop is detailed in the following section.

6.2 Data Collection

The workshop for validating FISM against the design criteria took place on 25 April 2016. The proof of concept of FISM, which was the focus of the workshop, is in the form of a spreadsheet-based supporting toolset. This workshop setting was used as it provides a good platform from which to not only demonstrate the supporting toolset to local government officials but also to provide the means for interaction and engagement with the toolset. Thus, the workshop attendees completed a guided walkthrough exercise of the functionality of the supporting toolset, with extensive opportunity for discussions and asking questions.

The workshop was attended by 20 municipal officials from several municipalities across the Eastern Cape of South Africa. All municipalities in the Eastern Cape that are in relatively close proximity to the location of where the workshop was facilitated were invited to send representatives to the workshop. However, the workshop venue only had capacity to facilitate a maximum of 20 municipal representatives. The group of municipal officials that attended the workshop represented several different functions of their respective municipalities. The number of attendees is listed in Table 6.1 according to their job title, along with the accumulative years of experience amongst attendees for a specific job title.

Table 6.1: Description of Demographics of Workshop Attendees

Job Title	**Accumulative Years of Experience in Position**	**No. of Attendees**
IT Manager	34+	7
Information Security Officer	3	1
IT System Administrator	17+	6
IT Technician	11+	4
Internal Audit and Risk Management Officer	4	2

The workshop attendees had a diverse range of skills and responsibilities, as listed in Table 6.1. Furthermore, this group of 20 municipal representatives shared an accumulative amount of experience within their positions in their respective municipalities in excess of 70 years. Most notably, the seven IT Managers boasted collective experience in excess of 34 years, while six IT System Administrators shared 17 and a half years of experience. However, the amount of experience within the group does not substitute the lack of resources that exists in their respective municipalities. This is because most municipalities that were represented at the workshop are classified in the category of low capacity, poor resource municipalities. Nevertheless, the large amount of experience does provide a reliable judgement on this validation of FISM.

The workshop attendees participated in hands-on exercises with the toolset, before providing input for the validation of FISM in a questionnaire. The toolset was designed to depict the process of FISM in a practical and simple way. Hence, the toolset lists the 'categories' and 'controls' of ISO/IEC 27002 along with descriptions thereof to the participant. These categories are then carefully considered and by process of elimination the relevant categories are selected for implementation. However, the categories in and of themselves cannot be implemented generically, as each category might consist of several underlying controls. Therefore, upon selection of the categories, their corresponding controls are presented in similar fashion for careful deliberation. Once all relevant categories and controls are selected, the toolset automatically generates a customised MISP that is based on the unique selections provided by the participant.

As mentioned before, to complete the validation exercise the attendees completed a questionnaire (see Appendix B). This questionnaire aimed at evaluating to what extent FISM adhered to the design criteria for the artefact of this study. The questions that evaluated these criteria were presented as statements upon which the respondents indicated on a Likert Scale to which extent they agree or disagree with that statement. Each statement, along with the question number is listed in Table 6.2, organised according to the criterion the questions are testing for.

The questions listed in Table 6.2 were supplemented by three open-ended questions. These open-ended questions aimed to determine how the

Table 6.2: Criterion Tested for by Questions of Questionnaire

Criterion	**Question No.**	**Statement**
HOLISTIC	2	In general, the topic of Information Security Management is comprehensively covered throughout the Information Security Management spreadsheet-based tool process.
SCALABLE	4	The Information Security Management spreadsheet-based tool allows Information Security Management to be implemented in a manner that scales to the size and resource capacity of any municipality.
	6	The Information Security Management spreadsheet-based tool can be equally successful in both larger and smaller municipalities.
SIMPLISTIC	3	It is possible to complete the exercises in this Information Security Management spreadsheet-based tool without extensive guidance or knowledge about the subject area.
	5	A person with limited technical ability would be able to successfully complete the exercises in this Information Security Management spreadsheet-based tool.
USABLE	1	The Information Security Management spreadsheet-based tool and its exercises could be readily implemented as is to function in any municipality.
	7	The Information Security Management spreadsheet-based tool would add value to a municipality if they implement it properly.

spreadsheet-based tool could be improved, what aspects of it were good and if the workshop attendees felt anything was missing completely. The results for each of the individual criterion will be discussed in the following section.

6.3 Data Analysis and Results

The analysis of the questionnaires and its results are crucial in determining whether or not FISM adheres to the design criteria argued in Chapter 3. The results of each criterion will, however, be reported on in individual subsections in no particular order.

6.3.1 Results on the Scalability of FISM

Both questions 4 and 6 aimed to measure the extent to which FISM meets the criterion of being SCALABLE. The results of this criterion of FISM being SCALABLE are depicted in Figures 6.1 and 6.2, respectively.

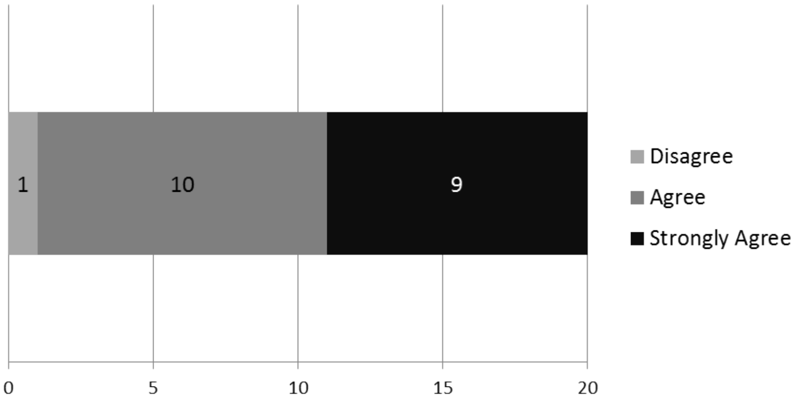


Figure 6.1: Results of Question 4

From Figure 6.1, it is clear that 19 out of 20 of the respondents agreed that the supporting toolset would scale well to municipalities of varying capacity and resource categories.

From Figure 6.2, it is clear that the overwhelming majority of respondents agreed that the spreadsheet-based tool can be successfully implemented in both large and small municipalities.

6.3.2 Results on the Usability of FISM

From Table 6.2, it is clear than the criterion of being USABLE, is tested for by questions 1 and 7. The results of the usability of FISM within municipalities are depicted in Figures 6.3 and 6.4, respectively.

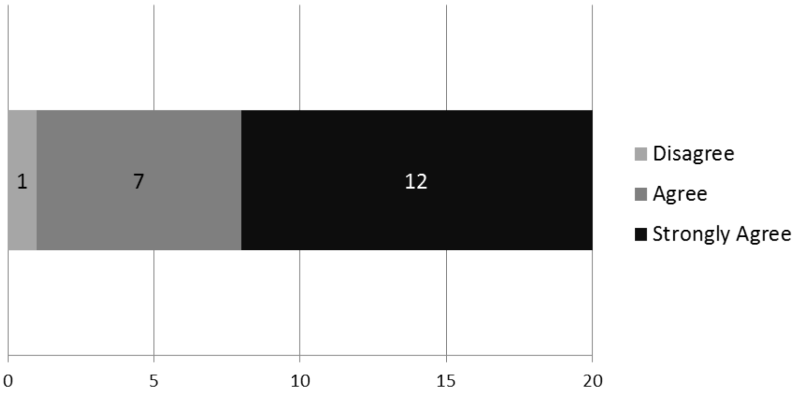


Figure 6.2: Results of Question 6

The consensus of the question, as depicted in Figure 6.3. is that all respondents agreed that the spreadsheet-based tool would be functional within municipalities without any adjustments or improvements.

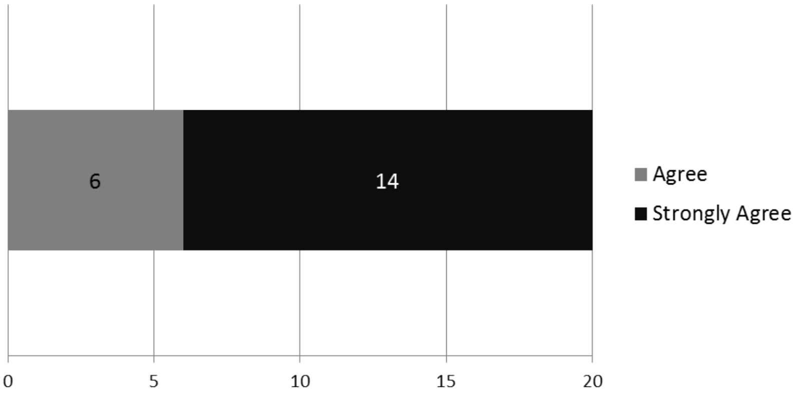


Figure 6.3: Results of Question 1

Once again, as seen in Figure 6.4, all of the respondents were in unison as they agreed mostly with strong conviction that the spreadsheet-based tool of the FISM would add value to any municipality if implemented properly.

6.3.3 Results on the Simplicity of FISM

The criterion of being SIMPLISTIC was tested for by both, questions 3 and 5. The results from these two questions are depicted in Figures 6.5 and 6.6, respectively.

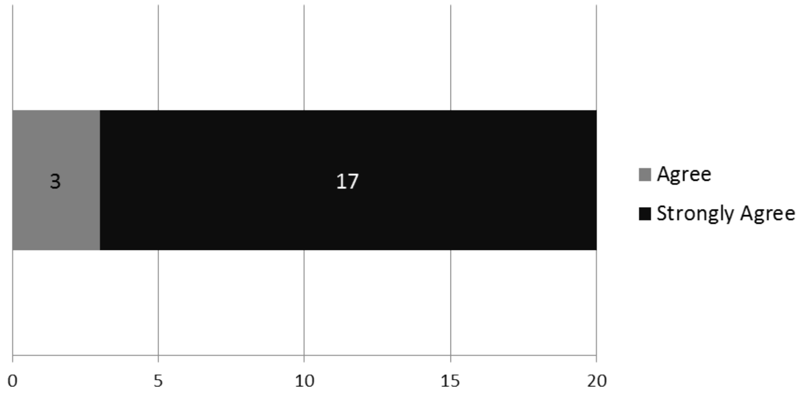


Figure 6.4: Results of Question 7

The results from question 3, as seen in Figure 6.5, clearly show that 14 out of the 20 respondents agreed that the spreadsheet-based tool of the FISM could be used without extensive additional guidance.

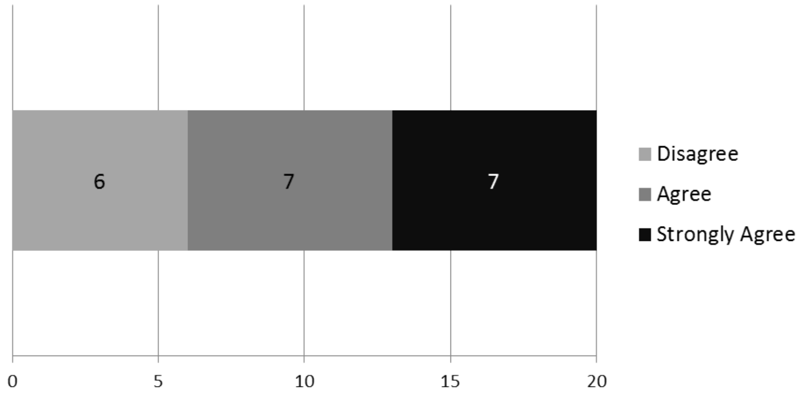


Figure 6.5: Results of Question 3

Figure 6.6, indicates that 15 out of the 20 respondents agreed that the spreadsheet-based tool of the FISM could be used by someone with limited technical knowledge and skills.

6.3.4 Results on the Holistic Nature of FISM

The final criterion of covering the topic of information security management in a HOLISTIC manner was tested for by question two of the questionnaire. The results of this question are depicted in Figure 6.7.

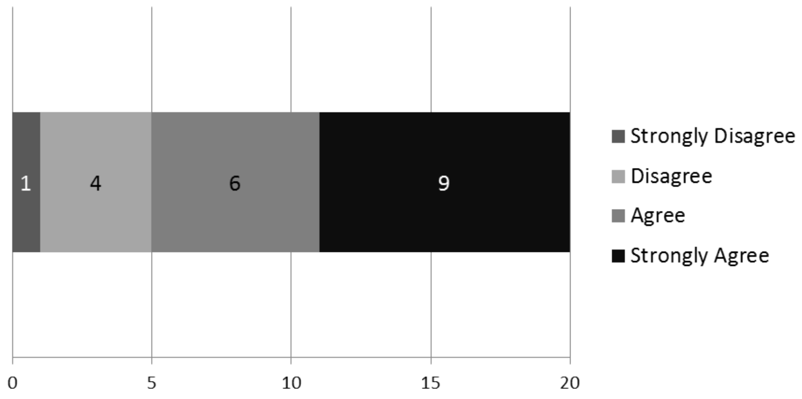


Figure 6.6: Results of Question 5

From Figure 6.7, it is clear that 19 out of 20 of the respondents agreed that the spreadsheet-based tool of the FISM covered the topic of information security management comprehensively.

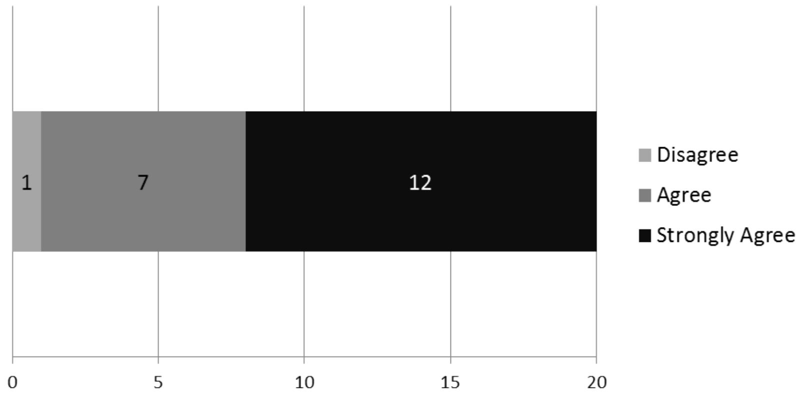


Figure 6.7: Results of Question 2

As for the additional feedback gained from the open-ended questions, several positive comments were made, as well as suggestions on how to improve this tool even further. There were some contradicting opinions with regard to the sufficiency of descriptions and detail provided by the tool as three different respondents commented:

- “At the moment I see no lacking (aspects/components) as the tool describes everything clearly and it addresses what needs to be done in order to address the problem area.”

- “More clarity on the objectives. The tool is straight forward and useful.”
- “The tool is highly complex and requires a lot of time to go through, it is, however, understandable due to the interlinking of the sheets.”

Furthermore, several respondents stated that they found specific aspects of the tool useful. Interestingly, these responses highlighted several aspects of the tool in the following manner:

- The ease to select applicable categories and get a ready MISP document for compliance.
- Excellent information and it will assist us.
- It touches on all important aspects of information security. The automation of the tool is genius work.
- The controls that can address the risk areas in a municipality. The security risk to be implemented are informed by the security requirements.

Another respondent made a notable suggestion to diffuse this tool so that all municipalities could access and use it in the following manner:

This again needs to be a web-based tool for on point updating.

The following section will discuss these results within the context of the research study as a whole.

6.4 Findings

The results from each question of the questionnaire have been discussed. However, the context and impact of these results on the study as a whole are still unclear. Therefore, the results will now be consolidated and reported on per criterion and not individual questions as before. Figure 6.8 illustrates the consolidated results of each criterion with a percentage value.

The criterion of being HOLISTIC received mostly positive responses, as seen in Figure 6.8. From this, it can be argued that information security management is covered comprehensively by FISM.

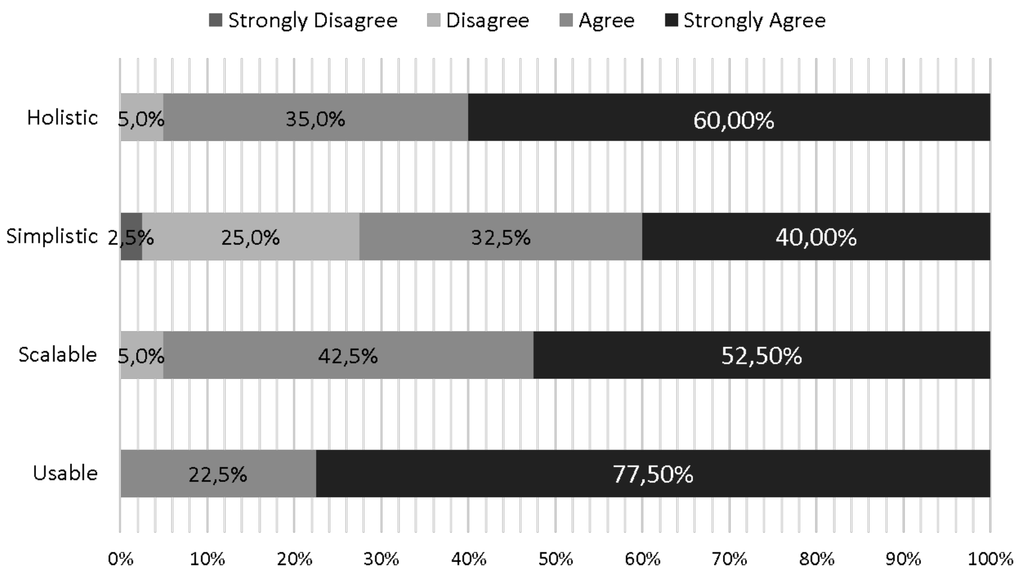


Figure 6.8: Consolidated Questionnaire Results per Criterion

As seen in Figure 6.8, the only criterion that received a response in the strongly disagree category was that of SIMPLISTIC. Furthermore, the criterion of SIMPLISTIC was the only one to receive disagree responses with a double digit value, at 25%. In order to understand this response, the researcher considered probable causes for it. The most probable cause is most likely linked to the fact that several of the respondents were not working in the ICT function of their respective municipalities. Thus, it could be that these individuals perceived the tool as not being SIMPLISTIC, due to their lack of knowledge in the field. However, the consensus of the criterion of SIMPLISTIC is predominantly positive. From the responses for the criterion of SIMPLISTIC, it can be argued that FISM is SIMPLISTIC enough to be suitable in the local government operating environment.

The criterion of being SCALABLE received mostly positive responses, as seen in Figure 6.8. From this, it can be argued that FISM caters satisfactorily to the varying needs of different municipalities and can scale well to their varying capacities.

The criterion of being USABLE within municipalities received overwhelmingly positive feedback, as none of the respondents opposed the integration of this criterion into the supporting toolset. Therefore, there should be no doubt that FISM is indeed suitable to be implemented within local government.

Considering the above, it can be concluded that the results of the validation workshop are that the supporting tool adheres to and incorporates all four criteria defined. This in turn, also implies that FISM adheres to these criteria, as the tool is merely a practical and more tangible illustration of FISM itself.

6.5 Conclusion

This chapter set out to discuss the validation of FISM against the design criteria it set out to adhere to. This validation exercise was completed via a workshop setting, which was attended by 20 municipal representatives. These municipal representatives came from various positions within their respective municipalities. This included several ICT managers, ICT system administrators, technicians and audit and risk officers. The group of municipal attendees of the workshop represented several municipalities from across the Eastern Cape province of South Africa.

The workshop served as a platform from which the attendees were presented with a theoretical foundation and practical supporting toolset of FISM, in the form of a spreadsheet-based tool. The attendees were provided with the opportunity to interact with the tool and a guided walkthrough of how it functions. Upon completion of the session, the attendees were asked to evaluate FISM by completing a questionnaire.

This questionnaire aimed at evaluating the extent to which the tool adheres to the design criteria of SCALABLE, USABLE, SIMPLISTIC and HOLISTIC. The seven questions were evaluated on a Likert Scale, to evaluate the degree to which the criteria are incorporated into the tool. There were also open-ended questions at the end of the questionnaire to gain additional feedback and insight.

The overall consensus was that the tool incorporated all four criteria, with very few instances of negative responses. Thus, the design criteria of this research study were adhered to in developing the FISM.

Chapter 7

Conclusion

The main objective of this chapter is to close the research study by drawing conclusions stemming from this study. This is done by firstly, summarising the essence and main findings from all preceding chapters. Consequently, a discussion follows in which the achievement of objectives is reflected upon. This is followed by a description of the key contributions made by this research study. Finally, possible future research is discussed before completing the dissertation with an epilogue.

7.1 Introduction

This chapter aims to report on the findings that stemmed from each individual chapter, the achievement of the research objectives, a summary of the contributions stemming from this study and a discussion of possible future research. The attainment of research objectives is vital to address the problem. However, in meeting the research objectives, several additional contributions originated from the study.

Each of the chapters within this research dissertation played an integral part in accomplishing the primary objective of this study, which was essentially to produce an artefact to address the identified real-world problem. Furthermore, the resultant artefact of this study is closely linked to the unique and specific context of this study. The main findings of each of the chapters, along with the role they fulfilled in the development, refinement and validation of the artefact will be discussed in the following section.

7.2 Summary of Findings

This study was introduced by focusing on the context within which this study is applicable. This introduction described both, the topic area of information security management and the context of this study, which is local government. The concerning status of information security management practices within the context of local government was discussed. This matter of concern led to the statement of the problem which this study aimed to address. Consequently, research objectives were formulated to address the problem at hand. These objectives consisted of a primary objective, which is collectively addressed by three secondary objectives. The primary objective of this research study was to develop an artefact which addresses the real-world problem (See Chapter 1).

One of the afore mentioned secondary objectives was to determine the minimum requirements of core components of information security management that is required for its sound implementation. The nature of information security risks was highlighted, along with its role in approaching the implementation of sound information security management. Information security policies were pointed out as core to managing information security and related risks. Furthermore, the importance of education, training and awareness initiatives was identified to be vital to the manifestation of acceptable information security behaviour in an enterprise. This was discussed in Chapter 2.

Chapter 3 started with a clear reflection of the current status of information security management practices within local government and pointed out that the situation at hand is very concerning. The biggest challenge local governments are faced with is that the majority of municipalities possess very little resources and adequately skilled personnel. Thus, in order to address this problem within local government, these specific challenges have to be overcome. The following criteria were argued to be vital aspects which should be incorporated into the artefact in order to overcome these challenges: SCALABLE, USABLE, SIMPLISTIC and HOLISTIC. If the artefact adheres to these criteria, it should be able to address the associated problem at hand in spite of the challenges local government face.

The primary research objective required this study to design an artefact to address a real-world problem. Thus, in order to accomplish this task, the research study followed the design-oriented IS research paradigm. This paradigm provides the researcher with academic freedom to the use of research methods, under the premise that the research adheres to the four research principles of this paradigm. The four principles are Abstraction, Originality, Justification, and Benefit. Furthermore, a new unique integrated research process was used for this study in order to conduct the research in this study. Chapter 4 discussed this research approach in detail.

The artefact that stemmed from this study is in the form of a framework, FISM (see Chapter 5). FISM consists of two components, which are; an Architecture and a Process, respectively. As prescribed by the unique integrated research process followed by this study, the initial draft of FISM underwent several refinement iterations before reaching the final version thereof. The Architecture component of FISM serves as the blueprint of WHAT needs to be in place within a municipality to effectively implement information security management. The Process component of FISM provides the necessary steps that details '*HOW*' achieve this effective implementation of information security management.

In order to validate to which extent FISM adheres to the criteria from Chapter 3, a workshop was conducted with 20 representatives of local government from the Eastern Cape province of South Africa. The Process component of FISM was presented to these representatives by means of a practical tool with which they could interact. This tool implemented the Process component to dynamically generate the ISPA; constituting the architecture component of FISM. A questionnaire was used to gather the necessary data in order to validate the adherence of FISM to the aforementioned criteria. The results showed that FISM did indeed adhere to the criteria set.

7.3 Meeting the Objectives

As argued in Chapter 1, the secondary objectives of this research study collectively contribute to addressing the primary objective of this study.

Secondary Objective 1

To determine the key contributing factors that hinder local government in implementing effective information security management

The first of these secondary objectives aimed to determine the challenges which local government faces with respect to its information security management practices, as well as possible factors that are a hindrance in this regard. This secondary objective is largely rooted within the discussions of Chapter 3. Chapter 3 highlighted that the most prominent challenge of local government in implementing sound information security management was the lack of resources and adequate skills in the majority of South African municipalities. Criteria were also argued by which the resultant artefact, FISM, could address these challenges. Therefore, by integrating these criteria into FISM, these challenges were not only identified, but also addressed in the mechanics of the framework. Thus, it can be argued that this secondary objective has been met.

Secondary Objective 2

To study standards and best practices to determine the key components of information security management that are relevant to local government

The second secondary objective was to study international standards and best practices related to information security management, in order to determine the core components of information security management that is vital to its sound implementation. These core components were described in Chapter 2 of this dissertation and formed the theoretical basis upon which FISM is based. Thus, this secondary objective has also been met as the resulting artefact was based on these core components.

Secondary Objective 3

To articulate a holistic approach by which local government can improve and adapt their individual information security management to align with their requirements

The third and final secondary objective aimed to articulate a holistic approach by which local government can improve its information security management practices. In essence, this secondary objective called for the actual development of FISM. To ensure that FISM provides local government with a holistic approach, FISM had to be based on generally accepted core components that coincide with international standards and best practices, but at the same time had to be constructed in such a manner that it addresses the unique challenges specific to local government. This objective was met by developing FISM by drawing from international standards and best practices portrayed in Chapter 2, while also adhering to the criteria argued towards in Chapter 3 to tailor the framework to the needs of local government. Thus, this secondary objective has been met by this research study.

The accomplishment of these three secondary objectives led to the formulation of the resulting artefact of this research, the FISM.

Primary Objective

To formulate a framework that will assist local government in South Africa, to implement sound information security management effectively

Thus, the primary objective has been met by collectively addressing the secondary objectives, which is evident in the successful development of FISM. The development process and the refinement iterations that FISM underwent are described in Chapter 5.

Although the development of FISM was the main contribution that would stem from this study, several additional contributions emerged along the timeline of the study. All contributions stemming from this study are described in the following section.

Although the secondary objectives and the primary objective have been met, the attainment of the methodological objective is yet to be discussed. As argued in Chapter 4, design-oriented IS research set four principles to be met by the artefact for this study to be deemed as truly design-oriented. Therefore, the four principles will be discussed, as well as how the artefact of this study adhered to each individual principle.

The four principles to which the artefact has to adhere to under design-oriented IS research are: Abstraction, Originality, Justification and Benefit, respectively.

Abstraction

Each artefact must be applicable to a class of problems

The first principle of Abstraction basically requires the artefact to be applicable to a group of problems, not a singular instance. It is evident that the resulting artefact of this study, FISM, is tailored to address information security management in all municipalities. It can be further argued that FISM is applicable to most enterprises in the South African context due to its foundation as it is founded upon international standards and best practices. Consequently, FISM can also be extrapolated to be applicable to other instances around the world. Thus, it can be argued that FISM fully adheres to the principle of Abstraction.

Originality

Each artefact must substantially contribute to the advancement of the body of knowledge

In order for the artefact to adhere to the principle of Originality, it needs to contribute to the advancement of the body of knowledge. Consequently, FISM is a tailor-made contribution that provides local government in general with guidance on how to implement sound information security management. One of the attendees of the validation workshop particularly supported this view by stating that: "At the moment I see no lacking (aspects/components) as the tool describes everything clearly and it address(es) what needs to be done in order to address the weak area." Thus, it can be argued that FISM adheres to the principle of Originality.

Justification

Each artefact must be justified in a comprehensible manner and must allow for its validation

The justification for this study is provided by the AGSA in that the lack of sound information security management practices of local government is deemed to be a great cause for concern. This in itself provides the basis on why FISM was developed. Furthermore, the principle of Justification requires that FISM should allow for its validation, which was done by means of a workshop. This workshop evaluated the integration of design criteria into FISM, as described in Chapter 6. Therefore, it can be argued that FISM adheres to the principle of Justification.

<u>**Benefit**</u>

Each artefact must yield benefit either immediately or in the future for the respective stakeholders

Concerning the last principle, design-oriented IS research requires the artefact to yield benefit to the relevant stakeholders group. Thus, in this study FISM should, therefore, yield benefit to local government. In Chapter 6, the benefit which FISM yields to a municipality was highlighted by the workshop attendees. This is evident in the numerous positive comments received during the workshop. One such comment was that FISM provides: "Excellent information and it will assist us." Another comment stated that: "It touches on all important aspects of information security. The automation of the tool is genius work." Thus, it is fair to argue that FISM adheres to the principle of yielding benefit.

Considering all of the above mentioned, this research study can indeed be classified as design-oriented IS research as the artefact, FISM, adheres to all four core principles. Thus, the methodological objective of adhering to the principles of design-oriented IS research has been met.

7.4 Summary of Contributions

The artefact of this research, FISM, was the premier contribution of this study. However, in the end, it was not the only contribution, as several academic papers stemmed from this study as well as a methodological contribution. All of which are described in the following subsections.

7.4.1 Research Contribution: The Artefact

The main research contribution of this study is undoubtedly the artefact, FISM. This is due to the fact that the primary objective of this research was to develop this framework towards information security management (FISM). FISM is constituted of two components. The first being Architecture and the second being a Process (see Chapter 5).

The Architecture proposes that an ISPA should be implemented and maintained as a bare minimum within any municipality. This ISPA consists of a MISP at a high level, with several supporting Municipal Information Security Standards which are typically issue-specific in nature. Furthermore, the ISPA of a municipality should stem from its unique and specific information security requirements.‘

In order to develop this ISPA, a specific Process is proposed by this study which forms the second component of FISM (see Chapter 5). This Process provides three steps that lead to the generation of an MISP, and its supporting information security standards, as required by the municipality. These two components collectively form FISM.

7.4.2 Methodological Contribution

The methodological contribution which stemmed from this study is the unique integrated research process it followed (as discussed in Chapter 4). This unique integrated research process was argued towards because of both, the lack of a detailed research process inherent to the paradigm, as well as the academic freedom the paradigm provides to pursue any logical approach to the study as long as the principles of the paradigm are adhered to.

This tailor-made approach is a four-phased process and is iterative in nature. This unique integrated research process can easily be used to provide detail on a methodological level for future similar research studies where the goal is to develop an artefact to address a real-world problem.

7.4.3 Academic Publications

Three academic publications stemmed from this study, of which two are international conference papers and the third, an academic journal paper.

The first written paper was accepted into the proceedings of the IST-Africa 2015 conference, which took place in Lilongwe, Malawi in May of the same year (see Appendix C). This paper was written in the very early stages of this study and focused largely on generating notoriety and support towards the issue of inadequate controls for information security management within South African local government. This paper also described the initial draft of FISM as described in Chapter 5.

The second paper that stemmed from this study was included in the proceedings of the subsequent IST-Africa conference of 2016, which took place in Durban, South Africa (see Appendix D). This paper reported on FISM after the completion of its second iteration of refinement, while FISM was not finalised yet. This paper also provided valuable input into the finalised version of FISM based on the feedback received from both, the reviewer(s) of the paper, as well as the conference delegates.

The third and final academic paper is a journal paper submitted to the South African Journal of Public Administration (JOPA) (see Appendix E). However, at the time of writing this dissertation, the paper was still under review. This paper described the finalised FISM, as well as the validation workshop exercise and its results.

7.5 Future Research

The context of this research was very specific and clearly delineated. Future research might prove beneficial if the artefact is extrapolated to a larger scope of context. This can easily be done as the artefact is based on generally accepted international standards and best practices.

Alternatively, the same scope and context might be used while extending or improving the artefact with additional components or possible improvements.

Another interesting development would be to see the results of a study which addresses the same problem within the same context, but from a completely alternate approach and research paradigm.

7.6 Epilogue

In any modern enterprise, information is a critical asset upon which all business operations rely. Thus, it is imperative for enterprises to adequately protect such information assets, which typically also include related ICT resources. For local government in South Africa, this is no different. However, the current status of information security practices in local government and its management is very concerning. Thus, this research study aimed to address the problem of inadequate controls for information security management that exists within local government.

In order to address this problem, this research study produced an artefact in the form of a framework. FISM, aims to provide local government with the necessary guidance to implement sound information security management. FISM comprises of two components, which are an architecture and an implementation process to supplement it. The architecture of FISM prescribes '*WHAT*' local government should have in place as a bare minimum in terms of information security management, while the process of FISM provides local government with the necessary steps on '*HOW*' to achieve this. Consequently, this research study achieved all of its objectives by producing this FISM in order to successfully address the problem at hand.

References

Auditor-General of South Africa. (2014). *Consolidated general report on the audit outcomes of local government 2012-13.*

Auditor-General of South Africa. (2015). *Consolidated general report on the audit outcomes of local government 2013-14.*

Belanger, F., & van Slyke, C. (2012). *Information Systems for Business: An Experiential Approach.* John Wiley and Sons, Inc.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*(May 2003), 1–9.

Cosic, Z., & Boban, M. (2010). Information security management - Defining approaches to information security policies in ISMS. *SIISY 2010 - 8th IEEE International Symposium on Intelligent Systems and Informatics*, 83–85.

Department: Public Service and Administration. (2012). *Public Service Corporate Governance of Information and Communication Technology Policy Framework.*

Department: Western Cape Local Government. (2015a). Local Government Circular: C5 of 2015.

Department: Western Cape Local Government. (2015b). *Municipal Corporate Governance of Information and Communication Technology Policy.*

Franklin, B. J., & Osborne, H. W. (1971). *Research methods: Issues and insights.* Wadsworth Publishing Company.

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. *Computers and Security*, *30*(8), 748–769.

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988.

Gerber, M., & Von Solms, R. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, *20*, 577–584.

Gerber, M., Von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security*, *9*, 32–37.

Herrington, J., McKenney, S., Reeves, T., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In *World conference on educational multimedia, hypermedia and telecommunications (edmedia) 2007* (pp. 4089–4097). (Appears In: Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2007)

Houde, S., & Hill, C. (1997). What do prototypes prototype. *Handbook of human-computer interaction*, *2*, 367–381.

Howell, W., & Fleishman, E. (1982). *Human performance and productivity, Vol 2: information processing and decision making.* Hillsdale, New Jersey: Erlbaum.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95.

IoDSA. (2009). *The King Report on Corporate Governance for South Africa.* Johannesburg: Institute of Directors for Souther Africa.

ISO/IEC 27000. (2012). *Information technology – Security techniques – Information securit management systems – Overview and vocabulary.* Geneva: ISO/IEC.

ISO/IEC 27001. (2013). *Information technology – Security techniques – Information securit management systems – Requirements.* Geneva: ISO/IEC.

ISO/IEC 27002. (2013). *Information technology – Security techniques – Code of practice for information security controls.* Geneva: ISO/IEC.

ISO/IEC 27005. (2011). *Information technology – Security techniques – Information securit risk management.* Geneva: ISO/IEC.

ISO/IEC 9241:11. (1998). *Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability.* Geneva: ISO/IEC.

IST-Africa Initiative. (2015). *IST-Africa Partners.* http://www.ist-africa.org/home/default.asp?page=partners. (Accessed: 5 July 2016)

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *Mis Quarterly Executive*, *9*(3), 163–175.

Longhurst, R. (2003). Semi-structured interviews and focus groups. *Key methods in geography*, 117–132.

McCumber, J. (1991). Information systems security: A comprehensive model. In *Proceedings of the 14th national computer security conference.*

Olivier, M. S. (2009). *Information technology research: A practical guide for computer science and informatics.* Van Schaik.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., & Sinz, E. J. (2010). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, *20*(1), 7–10.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers and Security*, *23*(8), 638–646.

Presidential Commissioners. (1998). *Report of the Presidential Review Commission on the Reform and Transformation of the Public Service in South Africa.*

Reeves, T. C. (2006). *Design research from a technology perspective* (Vol. 1). London: Routledge.

Republic of South Africa. (1996). *Constitution of the Republic of South Africa, 1996 - Chapter 2: Bill of Rights.*

SALGA. (2012). A Municipal Guide / Roadmap To Successful ICT Governance.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13.

Thomson, K. L., & Von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud and Security*, *2006*(5), 11–15.

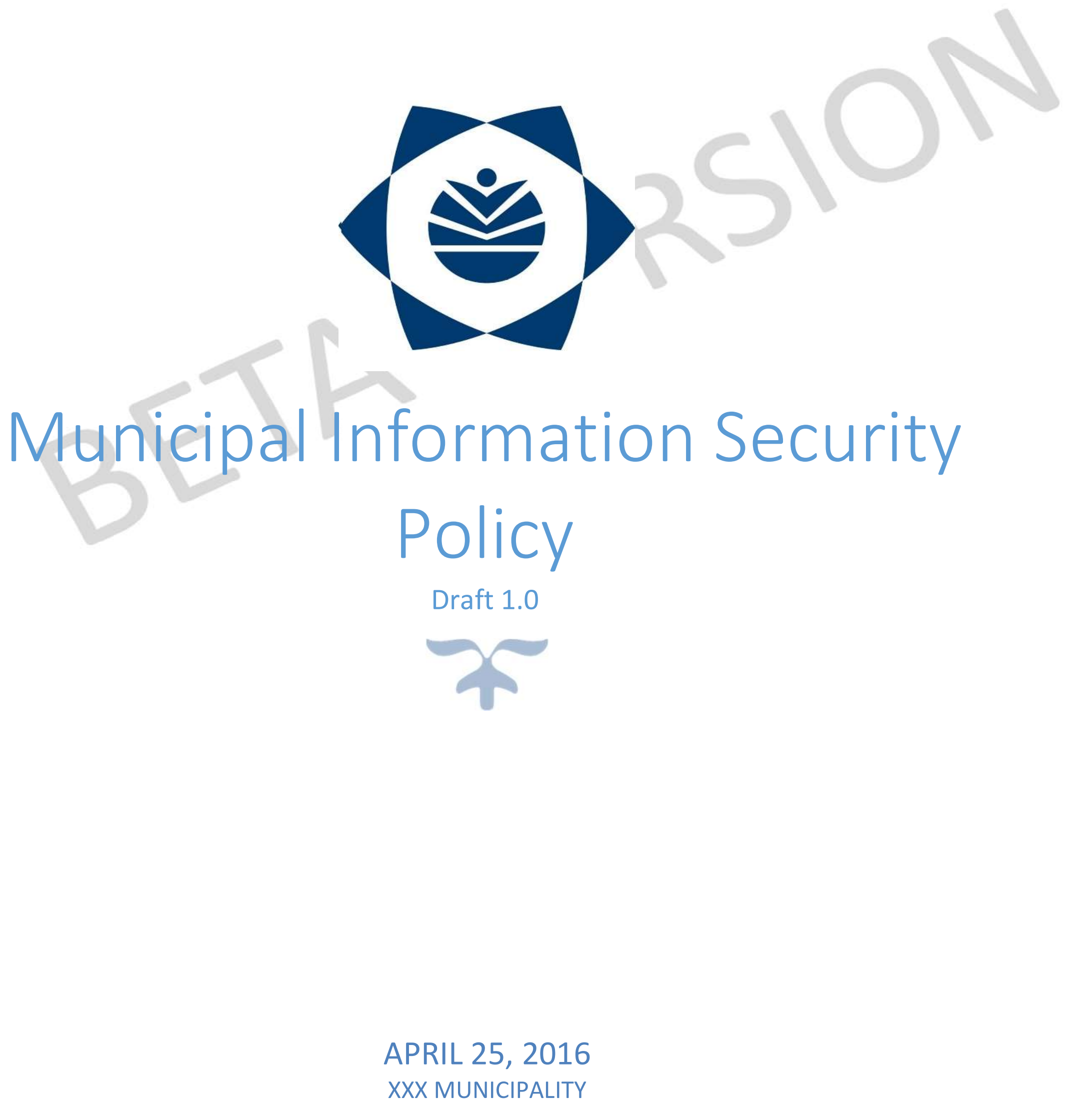
Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers and Security*, *23*(4), 275–279.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security.* Boston, USA: Cengage Learning.

Appendix A - MISP Example

Appendix A is an example of the Municipal Information Security Policy (MISP) that was generated upon completion of the toolset exercise of the validation workshop of the research study. This MISP shows all statements for the security categories as if all categories were selected for implementation by a municipality.



Municipal Information Security Policy

Draft 1.0

APRIL 25, 2016
XXX MUNICIPALITY

1. Introduction

Within <Municipality XX>, ICT is seen as a critical enabler for service delivery. The ICT systems of <Municipality XX> is used to process, store and transmit extremely valuable information on a daily basis. It is important that all information owned and processed by <Municipality XX> should be properly safeguarded to ensure that its confidentiality, integrity and availability remain intact. This policy document serves to provide the directives of the municipal council of <Municipality XX>, for the protection of its information, as it is essential to maintain effective service delivery, legal compliance and the reputation of <Municipality XX>.

Any employee, government entity or external party which makes use of or provides information resources to <Municipality XX> has a responsibility to maintain and safeguard them, and comply with the laws governing the processing and use of ICT. It is unacceptable for <Municipality XX> information resources to be used to perform any unethical or unlawful acts. Information Security is to be taken very seriously and it is expected to all employees to play their part in this regard.

The Executive Mayor of <Municipality XX> has ultimate responsibility and endorses the adoption and implementation of this Municipal Information Security Policy. Additional delegated roles and responsibilities are stipulated in Section 4.

This policy is designed to provide an appropriate level of protection to the information for which <Municipality XX> is responsible. The key aspects of this policy and all associated policies have been developed in accordance with the ISO/IEC 27002:2013 standard.

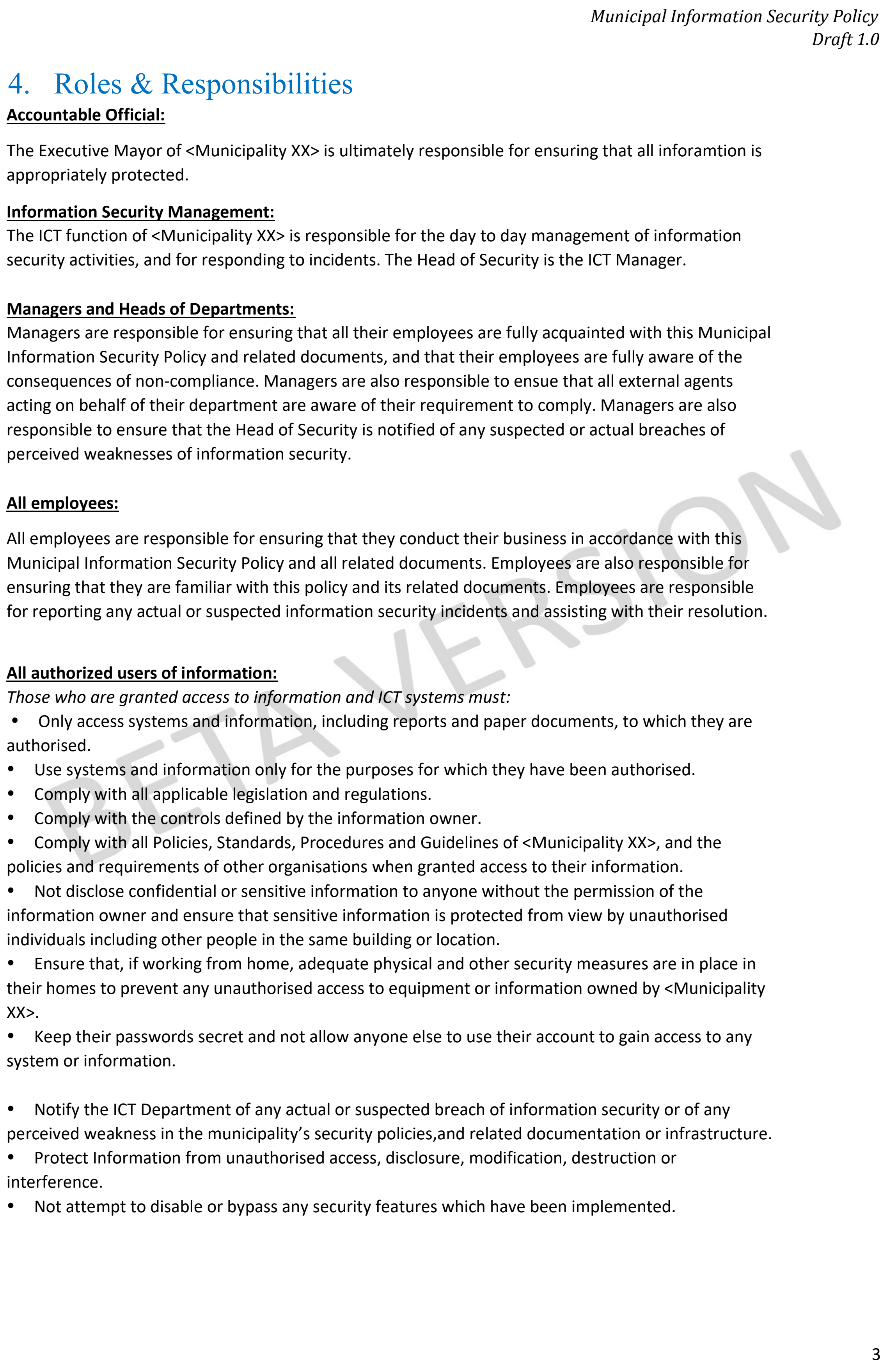
2. Objectives of Municipal Information Security Policy

The objectives of this Municipal Information Security Policy are to protect the information of <Municipality XX> by providing clear direction to ensure that:

- The ICT systems of <Municipality XX> are trustworthy and confidence in the accuracy and integrity of the information used and produced, is maintained in all users and the public.
- All users are aware of these policy statements and associated legal and regulatory requirements and of their responsibilities in relation to Information Security.
- Any unauthorised access, damage and interference to municipal premises, Information and ICT is prevented.
- Reputational and physical damage and interruption caused by security incidents are minimised.
- Unauthorised access to software and information is prevented.
- Confidentiality of personal and other sensitive information is assured.
- All legislative and regulatory requirements are met in relation to information assurance.
- The Council’s Information and ICT is used responsibly, securely and with integrity at all times.

3. Scope

This Municipal Information Security Policy applies to all employees, elected council members or other authorised users of the information of <Municipality XX>. The general public are entitled to view this policy document.



4. Roles & Responsibilities

Accountable Official:

The Executive Mayor of <Municipality XX> is ultimately responsible for ensuring that all inforamtion is appropriately protected.

Information Security Management:

The ICT function of <Municipality XX> is responsible for the day to day management of information security activities, and for responding to incidents. The Head of Security is the ICT Manager.

Managers and Heads of Departments:

Managers are responsible for ensuring that all their employees are fully acquainted with this Municipal Information Security Policy and related documents, and that their employees are fully aware of the consequences of non-compliance. Managers are also responsible to ensue that all external agents acting on behalf of their department are aware of their requirement to comply. Managers are also responsible to ensure that the Head of Security is notified of any suspected or actual breaches of perceived weaknesses of information security.

All employees:

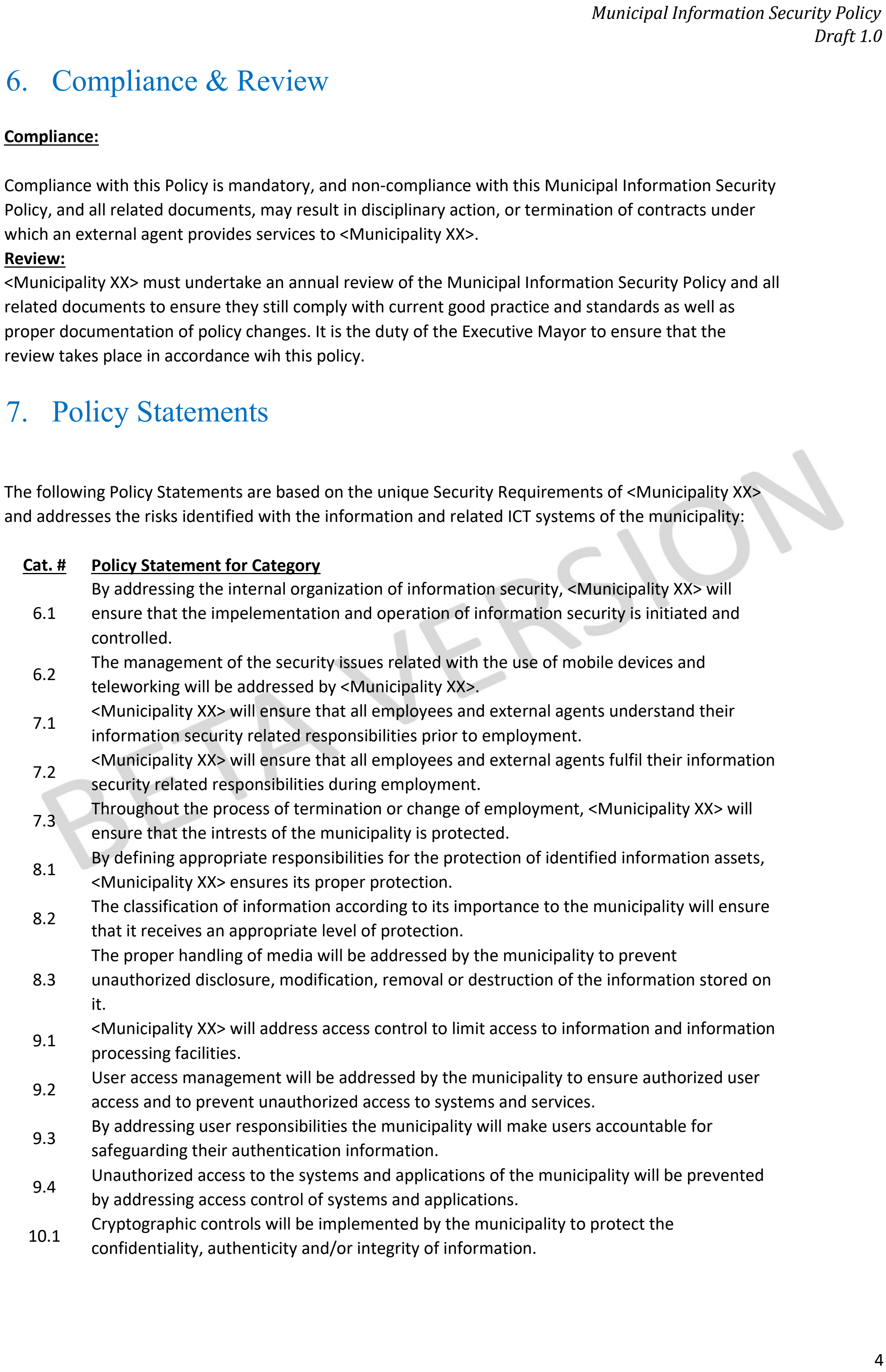
All employees are responsible for ensuring that they conduct their business in accordance with this Municipal Information Security Policy and all related documents. Employees are also responsible for ensuring that they are familiar with this policy and its related documents. Employees are responsible for reporting any actual or suspected information security incidents and assisting with their resolution.

All authorized users of information:

Those who are granted access to information and ICT systems must:

- Only access systems and information, including reports and paper documents, to which they are authorised.
- Use systems and information only for the purposes for which they have been authorised.
- Comply with all applicable legislation and regulations.
- Comply with the controls defined by the information owner.
- Comply with all Policies, Standards, Procedures and Guidelines of <Municipality XX>, and the policies and requirements of other organisations when granted access to their information.
- Not disclose confidential or sensitive information to anyone without the permission of the information owner and ensure that sensitive information is protected from view by unauthorised individuals including other people in the same building or location.
- Ensure that, if working from home, adequate physical and other security measures are in place in their homes to prevent any unauthorised access to equipment or information owned by <Municipality XX>.
- Keep their passwords secret and not allow anyone else to use their account to gain access to any system or information.

- Notify the ICT Department of any actual or suspected breach of information security or of any perceived weakness in the municipality's security policies,and related documentation or infrastructure.
- Protect Information from unauthorised access, disclosure, modification, destruction or interference.
- Not attempt to disable or bypass any security features which have been implemented.



6. Compliance & Review

Compliance:

Compliance with this Policy is mandatory, and non-compliance with this Municipal Information Security Policy, and all related documents, may result in disciplinary action, or termination of contracts under which an external agent provides services to <Municipality XX>.

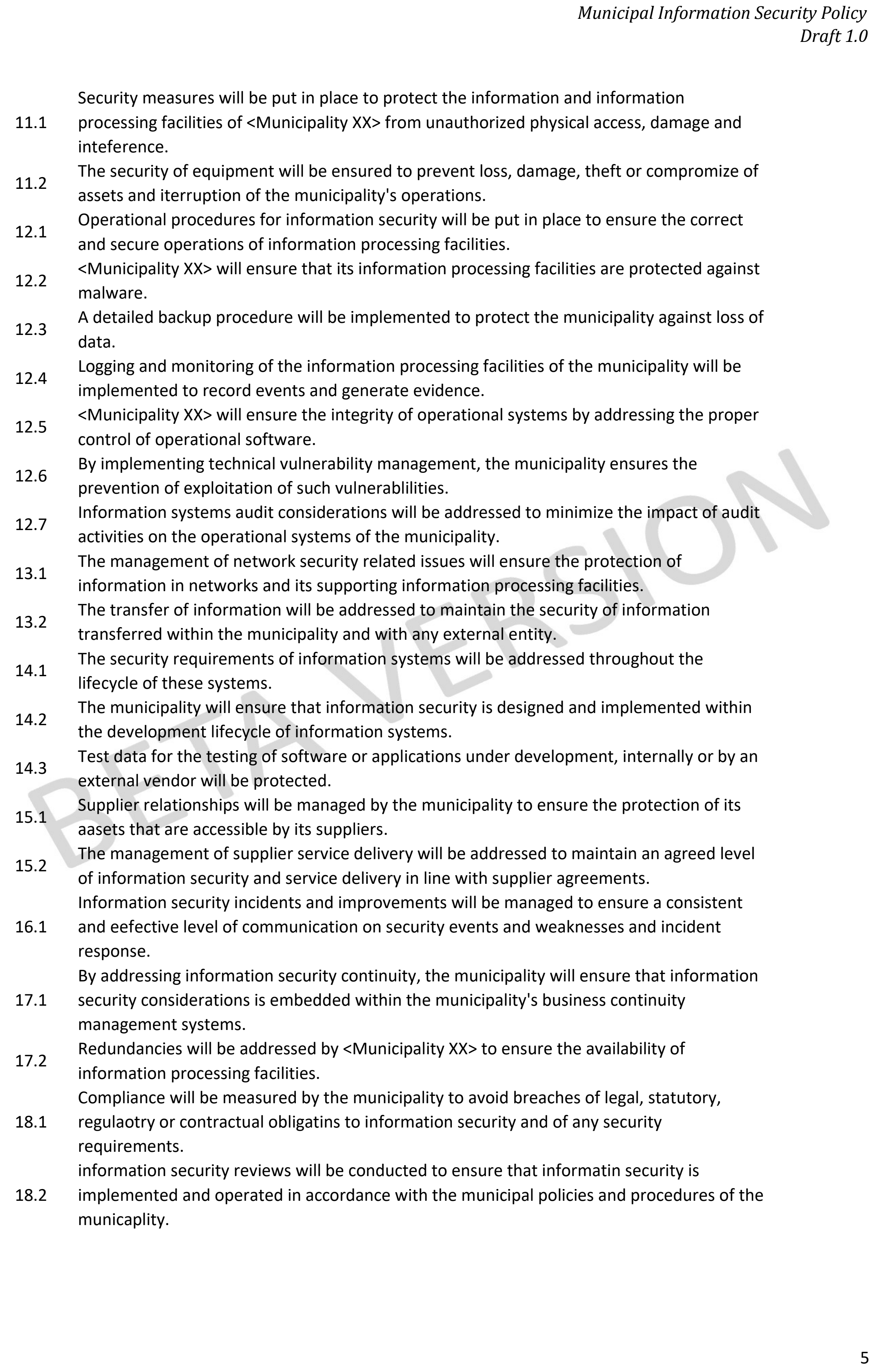
Review:

<Municipality XX> must undertake an annual review of the Municipal Information Security Policy and all related documents to ensure they still comply with current good practice and standards as well as proper documentation of policy changes. It is the duty of the Executive Mayor to ensure that the review takes place in accordance wih this policy.

7. Policy Statements

The following Policy Statements are based on the unique Security Requirements of <Municipality XX> and addresses the risks identified with the information and related ICT systems of the municipality:

Cat. #	**Policy Statement for Category**
6.1	By addressing the internal organization of information security, <Municipality XX> will ensure that the impelementation and operation of information security is initiated and controlled.
6.2	The management of the security issues related with the use of mobile devices and teleworking will be addressed by <Municipality XX>.
7.1	<Municipality XX> will ensure that all employees and external agents understand their information security related responsibilities prior to employment.
7.2	<Municipality XX> will ensure that all employees and external agents fulfil their information security related responsibilities during employment.
7.3	Throughout the process of termination or change of employment, <Municipality XX> will ensure that the intrests of the municipality is protected.
8.1	By defining appropriate responsibilities for the protection of identified information assets, <Municipality XX> ensures its proper protection.
8.2	The classification of information according to its importance to the municipality will ensure that it receives an appropriate level of protection.
8.3	The proper handling of media will be addressed by the municipality to prevent unauthorized disclosure, modification, removal or destruction of the information stored on it.
9.1	<Municipality XX> will address access control to limit access to information and information processing facilities.
9.2	User access management will be addressed by the municipality to ensure authorized user access and to prevent unauthorized access to systems and services.
9.3	By addressing user responsibilities the municipality will make users accountable for safeguarding their authentication information.
9.4	Unauthorized access to the systems and applications of the municipality will be prevented by addressing access control of systems and applications.
10.1	Cryptographic controls will be implemented by the municipality to protect the confidentiality, authenticity and/or integrity of information.



11.1 Security measures will be put in place to protect the information and information processing facilities of <Municipality XX> from unauthorized physical access, damage and inteference.

11.2 The security of equipment will be ensured to prevent loss, damage, theft or compromize of assets and iterruption of the municipality's operations.

12.1 Operational procedures for information security will be put in place to ensure the correct and secure operations of information processing facilities.

12.2 <Municipality XX> will ensure that its information processing facilities are protected against malware.

12.3 A detailed backup procedure will be implemented to protect the municipality against loss of data.

12.4 Logging and monitoring of the information processing facilities of the municipality will be implemented to record events and generate evidence.

12.5 <Municipality XX> will ensure the integrity of operational systems by addressing the proper control of operational software.

12.6 By implementing technical vulnerability management, the municipality ensures the prevention of exploitation of such vulnerablilities.

12.7 Information systems audit considerations will be addressed to minimize the impact of audit activities on the operational systems of the municipality.

13.1 The management of network security related issues will ensure the protection of information in networks and its supporting information processing facilities.

13.2 The transfer of information will be addressed to maintain the security of information transferred within the municipality and with any external entity.

14.1 The security requirements of information systems will be addressed throughout the lifecycle of these systems.

14.2 The municipality will ensure that information security is designed and implemented within the development lifecycle of information systems.

14.3 Test data for the testing of software or applications under development, internally or by an external vendor will be protected.

15.1 Supplier relationships will be managed by the municipality to ensure the protection of its aasets that are accessible by its suppliers.

15.2 The management of supplier service delivery will be addressed to maintain an agreed level of information security and service delivery in line with supplier agreements.

16.1 Information security incidents and improvements will be managed to ensure a consistent and eefective level of communication on security events and weaknesses and incident response.

17.1 By addressing information security continuity, the municipality will ensure that information security considerations is embedded within the municipality's business continuity management systems.

17.2 Redundancies will be addressed by <Municipality XX> to ensure the availability of information processing facilities.

18.1 Compliance will be measured by the municipality to avoid breaches of legal, statutory, regulaotry or contractual obligatins to information security and of any security requirements.

18.2 information security reviews will be conducted to ensure that informatin security is implemented and operated in accordance with the municipal policies and procedures of the municaplity.

8. Ownership of Policy

This policy document is owned by <Municipality XX>, and carries the full support and endorsement of the municipal council and the Executive Mayor of this municipality.

Signed By **Date**

Appendix B - Workshop Questionnaire

Appendix B is an example of the questionnaire used to evaluate the adherence to criteria of FISM. This is the questionnaire which was completed by the workshop attendees described in Chapter 6.

Nelson Mandela Metropolitan University
for tomorrow

Information Security Management in Local Government

Thank you for participating in the workshop session for Information Security Management. 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 Information Security Management spreadsheet-based tool and its exercises could be readily implemented as is to function in any municipality.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

2. In general, the topic of Information Security Management is comprehensively covered throughout the Information Security Management spreadsheet-based tool process.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

3. It is possible to complete the exercises in this Information Security Management spreadsheet-based tool without extensive guidance or knowledge about the subject area.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

4. The Information Security Management spreadsheet-based tool allows Information Security Management to be implemented in a manner that scales to the size and resource capacity of any municipality.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

5. A person with limited technical ability would be able to successfully complete the exercises in this Information Security Management spreadsheet-based tool.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

6. The Information Security Management spreadsheet-based tool can be equally successful in both larger and smaller municipalities.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

7. The Information Security Management spreadsheet-based tool would add value to a municipality if they implement it properly.

Strongly Disagree 😭	Disagree ☹	Agree 🙂	Strongly Agree 😁

8. What have you found to be particularly good and/or useful about the Information Security Management spreadsheet-based tool?

____

____

____

____

____

____

____

____

9. In what aspects, in your opinion, is the Information Security Management spreadsheet-based tool lacking?

____

____

____

____

____

____

____

10. In your opinion, what aspects about the Information Security Management spreadsheet-based tool can be improved?

____

____

____

____

____

____

____

____

Appendix C - IST-Africa 2015 Publication

*The first published paper is an international conference paper. The paper titled **'Better Information Security Management in Municipalities'**, was published in the proceedings of the 2015 IST-Africa international conference that took place in Lilongwe, Malawi.*

IST-Africa 2015 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2015
ISBN: 978-1-905824-50-2

Better Information Security Management in Municipalities

Joshua DE LANGE[1], Rossouw VON SOLMS[2], Mariana GERBER[3]
[1]*Nelson Mandela Metropolitan University,*
University Way, Port Elizabeth, 6001, South Africa
[1]*Tel: +27 71 898 1611, Email: s211087149@nmmu.ac.za*
[2]*Tel: +27 41 504 3604, Email: Rossouw.VonSolms@nmmu.ac.za*
[3]*Tel: +27 41 504 3705, Email: Mariana.Gerber@nmmu.ac.za*

Abstract: Municipalities handle valuable information in very large quantities on a daily basis. Due to the value, and often confidential nature, of this information, the protection of the information and the related technologies are a key concern for municipalities, especially in South Africa. For this very reason, several official government documents require South African municipalities to implement effective information security management systems. However, according to the Auditor General of South Africa, municipalities are struggling in this regard. This study uses a literature review, document analysis, and argumentation to identify the crucial components of an information security management system. These components are then logically presented in a hierarchical structure to possibly assist municipalities to improve their individual information security management processes. Addressing these components can also be applied in municipalities across Africa to improve information security management.

Keywords: Governance of Information Security, Information Security, Information Security Management, Information Security Policy, Municipalities, Municipal Council, ISO/IEC 27002 standard

1. Introduction

Information and Communication Technology (ICT) is a major contributor to effective service delivery in organisations across the world. Governments on the African continent have realised this fact, and are pursuing various avenues, in an effort to optimise their use of ICT, in order to enable their effective service delivery to the local population.

South Africa is governed at three levels: nationally, provincially and locally, as dictated by the Constitution, which is the supreme law in the country [1]. The mandate of local government is fulfilled by municipalities. The Constitution states that the objectives of local governments are [1]:

- To provide democratic and accountable government for local communities;
- To ensure the provision of services to communities in a sustainable manner;
- To promote social and economic development;
- To promote a safe and healthy environment; and
- To encourage the involvement of communities and community organisations in the matters of local government.

Furthermore, the functions and responsibilities of municipalities are to provide various services to the local citizens in the form of: electricity, water, sewage and sanitation, refuse removal, storm-water management, fire-fighting services, health services, land use and management, roads, public transport, street/informal trading, abattoirs and fresh produce markets, parks, as well as recreational facilities, library services and local tourism, according to the Constitution [1].

All of these services are nowadays rendered by utilising ICTs – to some extent. This statement is supported by the following extract from an official document of the Department of Public Service and Administration, the Corporate Governance of ICT Policy Framework (CGICTPF), as it states: “The purpose of ICT is to enable the Public Service in its quest for service delivery.” [2]. Thus, ICTs are critical in assisting municipalities to achieve better service delivery, and to highlight the importance of information within the context of municipalities in fulfilling their mandates to serve their people.

Thus, as municipalities rely heavily on information and related enabling technologies, the need to protect these resources properly is clearly a notable concern. The protection of information and related technologies is normally referred to as information security. When referring to information security, it is generally accepted that this term includes, not only the information itself, but also the technologies and systems involved with information processing, usage and transmission [3]. Three key elements collectively contribute towards the safekeeping of information in the context of information security: Confidentiality, integrity and availability. It is important that the process of information security be properly managed; and this is usually conducted through a process of information security management. The internationally recognised ISO/IEC 27000-set of standards directly addresses the management process of information security; and this will be discussed more extensively at a later stage in the paper.

Information security management is a key aspect in the good governance of ICT. This statement is supported by the King III Code [4], which is the most commonly accepted framework for Corporate Governance in South Africa; as it states that information security, information management and information privacy are to be properly addressed, in order to ensure that information assets are managed effectively [4].

The King III Code [4] was published in 2009; and it was the first of all the King Codes that dedicated an entire chapter to ICT and its governance. However, the Presidential Review Commission stated way back in 1998 that “all ICT decisions should come from Senior Political and Managerial leadership, and should not be delegated to technology specialists”. This was stated more than ten years prior to King’s inclusion of this concept in his code.

Nevertheless, despite the government’s best efforts, little improvement has been made in this regard. This fact has been reiterated by the Auditor General of South Africa in his investigations of both 2008/09 and 2009/10. Again in the 2012/13 findings, the Auditor General [5] stated that the “Status of information technology controls” is concerning; and it indicates that municipalities are struggling to effectively implement the necessary measures to improve the security of ICTs. More than half of the municipalities are yet to design controls for information security management; and a further 12% have controls designed; but they are struggling with the sustainable implementation thereof [5]. Another concerning fact is that user access management, a core element of information security management, is a big problem in municipalities; since 68% do not have any controls designed to address this aspect of security [5]. The Auditor General also pointed out that the confidentially, integrity and availability of information is largely in a concerning state; and the security of such controls is mandatory for ensuring information security [5].

From the above, it is clear that the general management of the security aspects of information and related technologies is generally not addressed properly in most South African municipalities. This is obviously a concerning situation; as highly valuable and sensitive information is processed in high quantities by municipalities; and the loss in the confidentiality, privacy and integrity thereof could result in disastrous consequences.

Therefore, the main objectives of this paper are to firstly, understand and assess the reasons for the current situation within municipalities in the context of information security management, by studying the literature and relevant documents. Secondly, the paper aims to propose an initial approach for improving information security management within municipalities – by proposing a series of steps in the form of a model that should improve the protection of information as a critical municipal asset.

The paper is aimed at municipalities in general, but specifically at managers who are responsible for the management of information security.

2. Research Approach

It is important when conducting research that the methods used in the research process are applicable and appropriate in the context of the study, and also that the methods lead to the results in a logical manner. The methods that are utilized in this research study include a literature review, a qualitative document analysis, and finally, argumentation towards an initial solution. As the cause for concern is within the municipal context, the recommendations of specific documents that apply directly to municipalities, in contrast to the comments of the Auditor General [5], have served as the core motivation for this study.

A literature review is described as being “a process of obtaining information relevant to your study”; and it is said to be “an iterative process” Olivier, [6]. Furthermore, Dodson [7] argues that a literature review consists of firstly identifying, secondly acquiring, and thirdly understanding just what is of relevance to the study, before writing up on the findings.

Therefore, this study initially aims to understand why the problem exists – by studying the relevant literature, specifically that in terms of municipalities and the state of their information security management systems.

A qualitative document analysis is an investigation that only focuses on current documents that already exist [8]; and it generally aims to understand the relevance of the document with relation to a predefined problem area [9]. Thus, the CGICTPF was studied, along with the ISO/IEC 27000-set of standards, as part of a qualitative document analysis.

The findings of this document analysis were compared to the annual findings of the Auditor General – in order to attempt to grasp the full extent of the problem.

Thereafter, a series of components that collectively address the problem was proposed, in order to enable the municipal council to know how to address the problem that municipalities face in implementing sustainable information security management controls. Tomhave [10] defines a model as being “an abstract, conceptual construct that represents processes, variables, and relationships”. Therefore, the above-mentioned components were logically presented in the form of a model.

3. Information Security Management and Best Practices

As mentioned earlier, the Auditor General’s reports between 2008 and 2010 highlighted that, in spite of the Presidential Review Commission’s (PRC) efforts in 1998 to inspire good governance of ICT within the sphere of local government, little improvement had been realised in more than ten years since the Presidential Review. This fact, along with pressure from best practices like the King III Code, which applies to municipalities, led the Department of Public Service and Administration of South Africa to create a legally binding document with which municipalities must comply on the Corporate Governance of ICT. This document, Corporate Governance of ICT Policy Framework [2], recommends that Information Security Management be addressed under the ISO/IEC 27000-set of standards. All of these documents, among others, will be discussed in the following subsection.

3.1 Relevant Best Practices

The King III Code is a best practice that addresses corporate governance on all the fronts of an entity, of which the governance of ICT comprise just one. The King III Code places the responsibility for strategic decision-making, concerning ICT governance, at the executive level. Furthermore, the accountability to ensure that these strategic ICT plans are executed effectively and sustainably also belongs to executive management. The King III Code dedicates a whole chapter to ICT governance, which should emphasise that it is a very important part of every business, in both the public and private sectors.

The King III Code in chapter 5, which addresses the governance of ICT, has 7 principles that are recommended as comprising good practice. The sixth of these principles is that "The board should ensure that information assets are managed effectively"; and this principle is broken down further into three elements, of which information security is one.

As mentioned earlier, the King III Code, in tandem with the PRC of 1998, and the AG findings of more than ten years later, indicated that little improvement had been made in governing ICT within local government. This fact led to the creation of the CGICTPF [2] by the South African Department of Public Service and Administration. The CGICTPF applies specifically to the various government departments of South Africa. This framework incorporates various approaches from different best practices and standards, like; the King III Code, ISO/IEC 38500, COBIT 5; and they also recommend the ISO/IEC 27000-set of standards for the implementation of information security management.

The CGICTPF was passed in December of 2012 as a legislative requirement to which all municipalities in South Africa must adhere [2]. Therefore, municipalities have no choice but to implement the recommendations of the CGICTPF; since it is mandatory to them. Thus, municipalities are also lawfully required, to address information security management in relation to the ISO/IEC 27000-set of standards.

The South African Local Government Association (SALGA) [11], which represents local government in many intergovernmental forums, published a further document in 2012 entitled: "A Municipal Guide / Roadmap to Successful ICT Governance" in support of the CGICTPF. This SALGA publication "provides suggestions on how to improve the status of ICT Governance within municipalities" and to assist the relevant parties to better understand and to familiarise themselves with the concept of ICT governance. This document extensively explains how different concepts within ICT governance apply in the municipal context; and again information security management is one of the key elements discussed in this document.

Both SALGA's publication [11] and the ISO/IEC 27000-set of standards recommend the creation of an Information Security Management System (ISMS), of which an effective Information Security Policy Architecture (ISPA) is a key element. Furthermore, a clear distribution of roles and responsibilities is needed to enable the effective implementation of an ISMS and ISPA, and also an understanding of ownership and accountability within executive management in the municipal sphere.

The ISO/IEC 27000-set of standards consists of several standards. However, the standards that will feature in this study are: the ISO/IEC 27000 [12] standard, the ISO/IEC 27001 [13] standard, the ISO/IEC 27002 [14] standard and also the ISO/IEC 27005 [15] standard. The ISO/IEC 27000 [12] standard serves as an introduction and scope to the rest of the set of standards; and it contains the general vocabulary used throughout the rest of the related standards, clearly explaining the use of various terms and phrases within the context of the set of standards. The 27002 [14] standard introduces various information security controls. In fact, it contains 114 security controls that fall under 14 Security Clauses and are categorised in 35 different security categories.

Not all the controls would be applicable in every entity; therefore, only those controls that apply to the intended target should be included in their ISMS. The ISO/IEC 27001 [13] standard serves as the standard against which organisations may seek independent certification of their ISMSs.

The ISO/IEC 27002 [14] standard specifies that information should be clearly classified under the “Asset Management Clause” [14] before there can be any attempt to secure it. In addition, the standard highlights the importance of a clear lay-out or understanding of the organisational structure before implementing an ISMS. The ISPA of the organisation, in this case a municipality, is recommended to clearly define expectations with regard to information security in a vast scope, ranging from human-resource security, to physical security, to relations with external parties.

Therefore, it may be stated that it is in a municipality’s best interest to implement these processes and controls to the best of their ability. If the implementation is effective and sustainable it would most likely result in considerable improvements with regard to the governance of ICT; and this would, in turn, cause the Auditor General’s annual findings to also reflect this progress.

The following subsection will put these best practices and aspects of information security management into the context of the previously identified problem situation.

3.2 Best Practices Related to the Current Status of Information Security in Municipalities

As mentioned before, the situation in South Africa with regard to information security management is very concerning; and it seems to be relatively stagnant. Little improvement is being realised; as the Auditor General adversely reports on information security controls within municipalities, year after year. Furthermore, numerous best practices were mentioned; and their relevancy to the municipal sphere was explained. The relationship between these best practices and the problem within the local government structure will briefly be explained.

The CGICTPF [2] requires of municipalities to create an environment of good governance; and it closely relates this to the principles of the King III Code. However, this is not being sustainably implemented; as 97% of municipalities, according to the Auditor General, are struggling to effectively implement the governance controls that they have designed [5]. Both CGICTPF and the King III Code recommend the ISO/IEC 27000-set as the ideal guideline for implementing information security management. The SALGA [11] publication also supports this recommendation; as most of its own recommendations concerning information security management are based on the ISO/IEC 27000-set of standards.

An effective municipal information security policy and good supporting policies are two of the most crucial aspects of a good ISMS. These policies should be directives that come from the municipal council; and a proper monitoring process should accompany these policies. Therefore, proper awareness of the roles and responsibilities among members of the municipal council is needed to ensure the effective implementation and functioning of these policies. Additionally, a clear understanding of the benefit of effective information security management is also crucial; and it would form part of any good ISMS.

However, ICT risks should be effectively managed by the municipal council to ensure that the municipal council has applied due care and due diligence in implementing the mandatory ISMS, as dictated by the CGICTPF [2]. Other factors that could contribute to the better management of information security within municipalities are a clear set of security requirements for each individual municipality. These security requirements should be created by considering various inputs, such as: legal and regulatory requirements, the results of a proper ICT risk analysis, and the strategic plans of the municipality, which comprises the Integrated Development Plan (IDP), of a municipality.

In spite of many regulatory requirements, and legislature demands that municipalities face, municipalities are still struggling with implementing sustainable ICT controls, according to the annual reports of the Auditor General. Therefore, the following section will propose a series of steps that would assist municipalities in addressing the problem situation.

4. Towards Better Information Security Management in Municipalities

From the previous section, it is clear that in order for municipalities to improve the process of information security management, there are several components that need to be considered when approaching the implementation or improvement of an ISMS. These components will be addressed in this section; and they will be arranged in a logical diagram. The diagram will clearly indicate from whence certain processes receive input, and alternatively provide input to other processes within ISMSs.

In the following diagram, the critical elements that are needed for municipalities to improve their ISMS are shown in a hierarchical order.

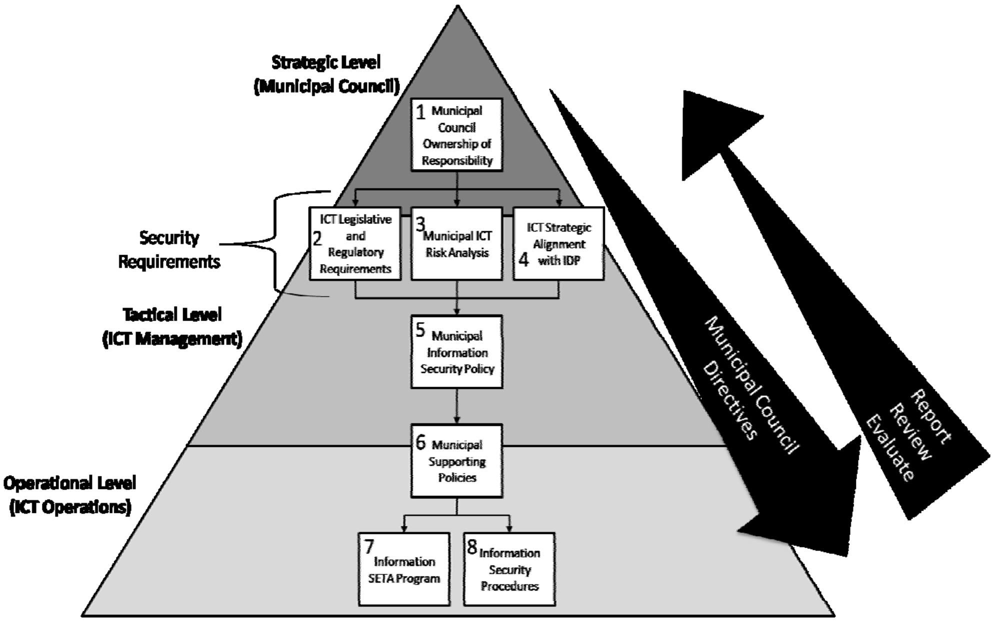

Strategic Level
(Municipal Council)
1 Municipal Council Ownership of Responsibility
Security Requirements
2 ICT Legislative and Regulatory Requirements
3 Municipal ICT Risk Analysis
4 ICT Strategic Alignment with IDP
Tactical Level
(ICT Management)
5 Municipal Information Security Policy
Operational Level
(ICT Operations)
6 Municipal Supporting Policies
7 Information SETA Program
8 Information Security Procedures
Municipal Council Directives
Report Review Evaluate

Figure 1: Critical Components of an Effective ISMS

There are eight components identified in the diagram above that contribute to an effective ISMS. These eight components will be discussed in the following subsections; and they will be addressed in numerical order, as indicated in the diagram above.

4.1 Municipal Council Ownership of Responsibility

Firstly, the municipal council must accept responsibility for information security, according to the CGICTPF [2] and King III [4]. After taking ownership of this responsibility, the municipal council should also understand their role in the information security management process. Part of the responsibility of the municipal council in every municipality is to determine what the security requirements are for that municipality.

These security requirements, according to the ISO/IEC 27002 standard [14], that logically follow this acceptance of responsibility by the municipal council, consist of three components, as seen in the above diagram: components 2, 3 and 4. These three components respectively provide input to clearly plotting the security requirements of individual municipalities by the municipal council; and they will be addressed in the following three subsections.

4.2 ICT Legislative and Regulatory Requirements

To comply with the legal and regulatory requirements regarding ICT, in the context of municipalities, is of the utmost importance. In approaching the governance of ICT, municipalities are required by law to comply with the CGICTPF [2]. In addition to the CGICTPF, SALGA published a document to assist municipalities in governing ICT, as well as implementing sustainable ICT controls, of which information security management is a key element. Information security is to be addressed under the guidance of the ISO/IEC 27000-set of standards, according to these documents.

4.3 Municipal ICT Risk Analysis

In the process of establishing the security requirements for a municipality, municipal councils have to consider the risks related to ICT. The ISO/IEC 27005 standard [15] is the best practice to be used by municipalities when performing risk analysis. Therefore, a proper ICT risk analysis is necessary to identify the risks and to evaluate their impact on ICT. These risks should also be evaluated to determine which risks are acceptable and which risks need to be addressed. To address these risks, the results of the risk analysis process must be considered in establishing the security requirements.

Although the municipal council are responsible for this risk management process, they are not required to physically implement or even design the controls that would mitigate the identified risks. However, the council should oversee that this is actually being done.

4.4 ICT Strategic Alignment with IDP

The importance of the strategic alignment of ICT with the long-term strategic goals of a municipality is evident in the fact that both the CGICTPF [2] and King III [4] promote this process as a crucial stepping-stone towards the good governance of ICT. The ICT strategic goals of a municipality should include goals specific to information security management. Thus, in order to improve the process of managing information security within a municipality, the municipal council should incorporate these strategic considerations when establishing the security requirements.

Therefore, the security requirements of a municipality should collectively be derived from considerations relating to three different components. These three components are: Strategic alignment, risk analysis and legislative requirements. The municipal council is responsible for initiating the process of establishing security requirements. However, the municipal council would not necessarily have to perform the underlying processes themselves. On the contrary, they should merely ensure that these contributing processes are in fact performed, and generate the security requirements resulting from these processes. The security requirements should, in turn, influence the content of the municipal information security policy.

4.5 Municipal Information Security policy

The municipal information security policy should be created in accordance with the security requirements of the municipality. The security requirements will indicate the type of behaviour that the municipal council expects from its employees regarding information security. This expectation of the municipal council should be embedded in this strategic level policy. Therefore, the purpose of the municipal information security policy is to translate the behavioural expectation of the municipal council concerning information security to its employees. Thus, in order to best translate this expectation, the structure of this policy is crucial.

There are certain elements that are mandatory in such a high-level information security policy, according to ISO/IEC 27002 [14]. The ISO/IEC 27002 standard [14] recommends that statements concerning the following topics must be included in such a high-level information security policy:

- "Definition of information security, objectives and principles to guide all activities relating to information security;" [14]
- "Assignment of general and specific responsibilities for information security management to defined roles"; [14]
- "Processes for handling deviations and exceptions." [14]

From the above, it is clear that, among others, the municipal council is required to address information security in this policy by clearly allocating information security roles and responsibilities throughout the municipality, as well as the behavioural expectations of the municipal council concerning information security. Furthermore, the above standard [12] recommends that this policy should contain some form of a compliance clause. The compliance clause of this policy should indicate how compliance to the policy would be determined and measured, as well as the expected consequences in failing to comply with the policy. The municipal information security policy should be supported by sub-policies that are more specific and that address various topics in more detail, as required by the municipal council.

4.6 Municipal Supporting Policies

These sub-policies that should be in place to support the high-level municipal-information security policy should address specific topics within information security. The ISO/IEC 27002 standard [14] states that examples of such topics might be:

- Access control
- Information classification
- Physical and environmental security
- End-user-oriented topics, such as:
  - acceptable use of assets
  - clear desk and clear screen
  - information transfer
  - mobile devices and teleworking
  - restrictions on software installations and use
- Back-up
- Protection from malware
- Management of technical vulnerabilities
- Cryptographic controls
- Communication security
- Privacy and protection of personally identifiable information
- Supplier relationships

Therefore, the municipal council should oversee the creation of several supporting policies that address such relevant topics. Those topics that need to be addressed could be different for individual municipalities; as the security requirements for municipalities would also be unique. Firstly, the municipal council should ensure that all the employees and external parties involved with the processing of municipal information are aware of, and understand these policies. Secondly, the municipal council should ensure that the supporting policies are related to step-by-step procedures to enable compliance with the municipal-policy architecture.

4.7 Information SETA Program

As previously mentioned, in order for the municipal council to ensure awareness of, and a clear understanding of its ISPA, an information security education, training and awareness (SETA) program should be implemented. The SETA program should especially be focused on continually raising awareness of the topics that are addressed by the municipal-supporting policies.

Once awareness is raised on a topic, employees would be more willing to be trained and educated with regard to the topic. Properly trained and educated staff would, in turn, relate to the more effective execution of information security procedures.

4.8 Information Security Procedures

Finally, the municipal council should, as previously mentioned, ensure that the municipal information security architecture is translated into relevant and comprehensive information security procedures. These procedures should indicate to the relevant staff members of the municipality exactly how to perform the tasks expected of them, as dictated by the municipal policies that govern information and its management.

Thus, the purpose of these procedures is to enable the sustainable implementation of an effective ISMS.

As mentioned before, the ideal set of controls that would contribute to better information security management in municipalities would be information security procedures, along with continuous efforts to raise awareness of the information security policies within the municipality. This is clearly indicated in the diagram, as these two components are at the operational level of the municipal structure. Being at the operational level, these two components are the responsibility of all parties involved with the processing of municipal information.

Furthermore, as the diagram indicates, information security procedures and the SETA program emanate from the municipal-supporting policies. These supporting policies, in turn, find their origin in a high-level municipal information security policy. The municipal information security policy is created in alignment with the municipality's security requirements. However, the municipality's security requirements should be established by the municipal council once they accept ownership of the responsibility for information security management within the municipality, as is required by law.

5. Conclusion

As stated earlier, the first objective of the paper was to investigate the literature and relevant documents in the context of municipalities and ICT, and more specifically information security management. This literature study and document analysis indicated that information security management is a crucial concern for municipalities, as they are not meeting the mandatory requirements set by government leadership. This shortcoming is evident; as more than half of the municipalities in South Africa have no controls designed concerning information security management [5]. To address this problem, documents like the CGICTPF [2] and SALGA [11] were analysed to determine what is legally required of municipalities concerning information security management. After this analysis, the requirements were compared to the current status of information security management efforts by municipalities, as described in the findings of the Auditor General.

Finally, in an effort to assist municipalities in improving their information security management, key components of an effective ISMS were presented. These components were logically presented in the form of a model. If municipalities are to address these components, a considerable improvement should be seen in the process of managing information security.

Although this study is ongoing, the current discussion in this paper is based largely on the literature, and specifically on documents like SALGA, CGICTPF and the audit results, in order to investigate the current situation within municipalities in the context of information security management. In the light of this issue, best practices and international standards, like the King III Report and the ISO/IEC 27000-set of standards, were analysed to propose an approach for improving information security management efforts within municipalities. The proposed framework is progressively being refined, as the case study proceeds. Thus, additional results will follow at a later stage due to continuation of the investigation as part of the case study, along with further analysis of these results.

References

[1] *The Bill of Rights of the Constitution of the republic of South Africa.* (1996). Government Gazette. (No. 17678).

[2] Department: Public Service and Administration. (2012, December). *Public Service Corporate Governance of Information and Communication Technology Policy Framework.* South Africa: the dpsa.

[3] Whitman, M. E. and Mattord, H. J. (2011). *Principles of Information Security* (4th ed.).

[4] IoDSA. (2009). *King Code on Governance for South Africa.* Johannesburg: IoDSA.

[5] Auditor – General of South Africa. (2013). *Consolidated general report on the audit outcomes of local government.* Auditor – General South Africa.

[6] Olivier, M. S. (2009). *Information Technology Research – A Practical Guide for Computer Science and Informatics* (3rd ed.). Pretoria: Van Schaik.

[7] Dodson, D. C., Secker, J. A., Scott, R. B. and Reeves, L. H. (2004). Retrieved from: http://www.soi.city.ac.uk/~dcd/pc/2004/litr/lit.pdf

[8] Scambor, E. A. (2002). *Guideline - Document Analysis.* Peerthink, 1–6.

[9] Mayring, P. (2000). *Qualitative Content Analysis.* Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1(2). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1089/2385

[10] Tomhave, B. L. (2005). Retrieved December 7, 2014, from www.secureconsulting.net/Papers/Alphabet_Soup.dpf

[11] South African Local Government Association. (2012, June). *A Municipal Guide / Roadmap To Successful ICT Governance.* South Africa: SALGA.

[12] ISO/IEC. (2014). *ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary.* Geneva, Switzerland: ISO/IEC.

[13] ISO/IEC. (2005). *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.* Geneva, Switzerland: ISO/IEC.

[14] ISO/IEC. (2013). *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.* Geneva, Switzerland: ISO/IEC.

[15] ISO/IEC. (2008). *ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.* Geneva, Switzerland: ISO/IEC.

Appendix D - IST-Africa 2016 Publication

The second published paper is an international conference paper. The paper titled ***'Information Security Management in Local Government'****, was published in the proceedings of the 2016 IST-Africa international conference that took place in Durban, South Africa.*

IST-Africa 2016 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2016
ISBN: 978-1-905824-54-0

Information Security Management in Local Government

Joshua DE LANGE[1], Rossouw VON SOLMS[2], Mariana GERBER[3]
Nelson Mandela Metropolitan University,
University Way, Port Elizabeth, 6001, South Africa
[1]*Tel: +27 71 898 1611, Email: s211087149@nmmu.ac.za*
[2]*Tel: +27 41 504 3604, Email: Rossouw.VonSolms@nmmu.ac.za*
[3]*Tel: +27 41 504 3705, Email: Mariana.Gerber@nmmu.ac.za*

Abstract: Information and Communication Technology (ICT) has become so pervasive in most organizations, that business functions are almost completely dependent on it. ICT is the platform that enables most of the organization's information processing and storage. Within the context of local government, this is also the case as ICT plays a crucial role in achieving their goal of service delivery to their communities. Due to its high importance, the information and related ICT systems should be adequately protected by the process of information security management. However, the problem remains that the efforts of local government in addressing information security is unsatisfactory. In order to address this, the objective of this paper is to propose an architecture, combined with a process model, which aims to assist local government to improve their information security management. This architecture and process model was refined by engaging with practitioners within local government and is not only applicable to South Africa, but also the rest of Africa.

Keywords: Information Security, Information Security Management, Information Security Policy Architecture, Municipalities, ISO/IEC 27002

1. Introduction

In the modern age, the important role that Information and Communication Technology (ICT) plays in organizations is undeniable. This importance is due to the fact that most operational processes rely on ICT systems to: transmit, process and store information [1]. Furthermore, it can be argued that the very success of the organization is dependent on information being readily available and that the integrity of this information be reliable, as well as the confidentiality of such information be ensured. These three elements namely: confidentiality; integrity; and availability, are conceptually what comprises information security [2].

Therefore, information security is a crucial component in the success of any organization, regardless of what environment the organization functions in. It is thus inevitable that local government, just like any other organization, need to address information security. However, it is imperative to understand the unique landscape of local government before addressing the issue of information security. The government of South Africa is divided into three spheres namely: national, provincial and local government [3]. Furthermore, local government consists of many municipalities that are further divided into the following three categories – metropolitan, district and local municipalities [3]. Every municipality, regardless of category, functions as an entity that is both interdependent and interrelated to other government institutions, yet individually represents a fully-fledged level of government to the community it serves.

South African local government is audited annually by an executive auditing body that is sanctioned by the national government to ensure accountability and transparency throughout government. This body, the Auditor-General of South Africa (AGSA), publicly publishes its findings within local government in an annual report. In the latest consolidated report of 2013/14, information security management was highlighted to be a big concern as the majority of local government failed to design or implement sustainable controls in this regard [4]. The role of controls in ensuring the security of information can be defined in the following manner: *"Information security is achieved by implementing a suitable set of controls"*[5]. These controls can be embodied in various forms, ranging from policies, processes and procedures to organizational structures and software and hardware functions[5].

The lack of adequate controls for information security is clear from Figure 1, as a combined 69% of municipalities, out of a total of 278 municipalities, are yet to either design or implement such controls. It is implied that these municipalities, that fall within the 69% that do not have adequate controls in place, are vulnerable to breaches of confidentiality, integrity or availability, or a combination of the three. Therefore, local government in South Africa have no way of evading the fact that they need to earnestly address the issue of information security management.

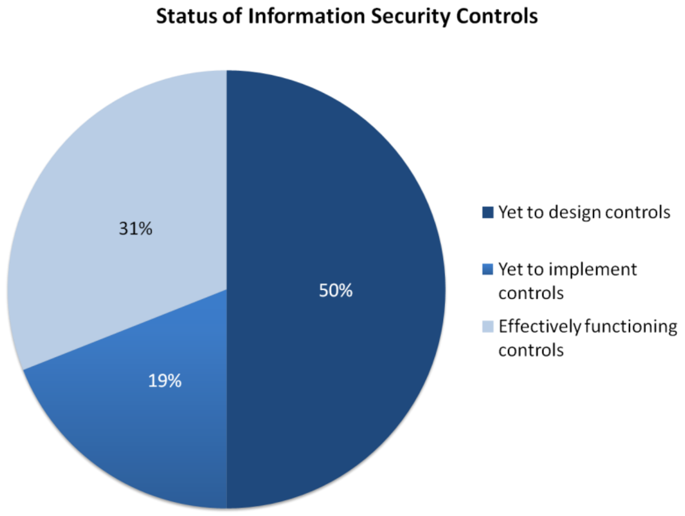


Figure 1- Findings on Information Security Controls Within Municipalities by the AGSA

Notwithstanding the above, even though it is very important, the problem that local government in South Africa is faced with is that their efforts towards information security remain unsatisfactory. Thus, the objective of this paper is to, not only introduce the reader to the challenges faced by local government in addressing information security management; but also, to propose a process to aid local government with improving their information security efforts.

The remainder of this paper will address the approach followed in completing this research, followed by a discussion to further contextualize the position of this research within local government in South Africa. After which, the reader will be introduced to the researcher's proposed process and underlying architecture, before reflecting on the achievement of the various objectives of this paper.

2. Research Approach

This paper constitutes a small portion of a bigger project that is yet to be concluded. The aforementioned research project follows a design-oriented approach, by which the researchers strive towards delivering a tangible artefact that can be utilized in practice [6]. The artefact of this research, which consists of both an architecture and process model, is the focus of this paper.

The research follows a cyclic approach for justification, whereby local government officials are consulted to provide feedback and input to refine the contribution presented by the researchers, which in this case is the architecture and process model. For the purpose of this research, the initial draft of any contribution is mostly based on findings from a literature review. The contribution is then verified and refined upon reception of feedback, predominantly in the form of semi-structured interviews, from local government. A semi-structured interview can be defined as *"a qualitative method of inquiry that combines a pre-determined set of open questions (questions that prompt discussion) with the opportunity for the interviewer to explore particular themes or responses further"* [7].

The initial draft of the architecture was the subject of such discussions during a visit to a district municipality in South Africa on 19 August, 2015; after which the necessary changes and improvements were then applied to the architecture. Along with the improved version of the architecture, an initial draft of the process model was presented to the above mentioned district municipality on 17 November, 2015; where semi-structured interviews was once again the method of engagement. Thus, both the architecture and process model presented in this paper have been refined and adapted after having been the subject of discussion during rigorous engagement with local government.

The line of argumentation in this paper is therefore, based on the results of a literature review, semi-structured interviews and the verification of the contribution. In the following section information security management will be discussed, followed by the current state of information security management within local government in South Africa.

3. Managing Information Security in Local Government

This section will commence with a discussion on information security practices and the management thereof. After which, the current efforts toward information security within local government will be discussed; followed by a focus on possible challenges with the current approach.

3.1 – Information Security Practices

As mentioned previously, information security predominantly aims to preserve the confidentiality, integrity and availability of information [8]. Gerber, Von Solms and Overbeek [2] define confidentiality in the following manner: *"Confidentiality refers to the property that information is not made available or disclosed to unauthorized individuals, entities, or processes."* Integrity however, can be defined as the property that aims to ensure that data is not altered or removed without the proper authorization [2]. Availability requires that data be readily available upon demand by all authorized individuals, entities, or processes [2]. However, for information security practices to be successful, these three aspects have to be protected holistically during various phases – transmission, processing and storage [1].

Furthermore, it is widely accepted that both technological controls and human behaviour are central aspects that need to be addressed when protecting information [9], [10]. In essence, all of the above mentioned factors are equally important when attempting to safeguard information. If information is not properly safeguarded by implementing adequate controls, the impact of both short- and long term information security breaches can have a devastating effect on an organization – and can even threaten the very survival of an organization. Thus, it can be argued that secure information is an absolute necessity to the success of any organization.

Accordingly, information security should be acknowledged as a strategic issue that needs to be addressed at the highest level. Consequently, the proper management of information security should become a key concern for all organizations. Considering the above mentioned, it is apparent that the management of information security can be a daunting undertaking due to the diverse nature of information security. However, information security and the management thereof can be considerably less intimidating by making use of readily available best practices and standards.

The standard that will be focused on in this paper is the ISO/IEC 27002 standard. It is important to note that this standard forms the largest part of the theoretical foundation on which the contribution is based that will be discussed in section 4, supported by related literature sources. It is stated in ISO/IEC 27002 that the aim of the standard is to guide organizations in implementing commonly accepted information security controls [5]. Currently, there are 114 controls within the standard for organizations to consider, divided into 35 security categories. Furthermore, the security categories are grouped across 14 main security clauses. The selection of these controls is entirely dependent on organizational decisions, stemming from strategic goals, risk assessments and the legal and regulatory landscape, and can vary from organization to organization [5]. Therefore, the unique nature of the operating environment of the organization plays a big role in this decision making process.

After an organization has completed this decision making process, a set of controls is ready for implementation. Typically the question remains – *where to from here?* The chosen set of controls is then translated into an information security policy architecture (ISPA) which in principle consists of a high-level information security policy – which is supported by sub-policies. These sub-policies, or company standards as they are sometimes referred to, are usually more focused on specific issues or topics within information security [11]. The organizational ISPA aims to ensure the safety of the organization's information and related assets, by dictating controls that are either technological in nature, or that aim to dictate human behaviour.

The clauses within ISO/IEC 27002 are generally orientated towards focusing on either addressing technological or the human aspect of information security. This correlation is depicted in Table 1, and will be followed by argumentation towards this position by discussing each clause within this context.

Table 1 - Orientation of ISO/IEC 27002 Clauses

Clause name	Technological	Human Aspect	Hybrid
Information security policies		✓	
Organization of information security		✓	
Human resource security		✓	
Asset management		✓	
Access control			✓
Cryptography	✓		
Physical and environmental security			✓
Operations security			✓
Communications security	✓		
System acquisition, development and maintenance			✓
Supplier relationships		✓	
Information security incident management		✓	
Information security aspects of business continuity management			✓
Compliance		✓	

The first clause, information security policies, focuses on addressing the human aspect of information security. Although technological controls are addressed in the ISPA of an organization, the policies aim to dictate human behaviour when they interact with the ICT systems – as well as stipulating acceptable conduct while handling any organizational information [5].

The second clause, organization of information security, is where roles and responsibilities for information security are defined and communicated to all relevant parties, as well as the acceptable use of mobile devices are dictated. Thus, this clause also aims to address the human aspect of information security [5].

The third clause, human resource security, aims to address information security issues relating to the employee before, during and after employment – as well as responsibilities and duties related to change of employment. Thus, this clause is also focused on the human aspect of information security, by aiming to protect the information of the organization during various phases of employment [5].

The fourth clause, asset management, also focuses on the human aspects of information security. The responsibilities for asset management, such as asset inventory, ownership and acceptable use, are defined within this clause. This clause also addresses the classification of information according to its importance to the organization. Furthermore, the clause also aims to govern the use, prevent unauthorized modification, disclosure or destruction of information on removable media and the access to such media [5].

The fifth clause, access control, addresses both the human and technological aspects of information security and is thus of a hybrid nature in this regard. This clause addresses the human aspect of information security by defining the business requirements of access control which includes: access to networks and systems, user registration and de-registration and the management and review of access rights. The technological aspect is addressed by advocating proper password management systems, secure log-on procedures and access control to program source code [5].

The sixth clause, cryptography, is technological in nature as it addresses the cryptographic controls that are needed to ensure the confidentiality, integrity and authenticity of an organization's information [5].

The seventh clause, physical and environmental security, addresses both the human and technological aspects of information security and is thus of a hybrid nature. In this clause, the securing of physical equipment, the organizational premises and protection from environmental threats are addressed [5].

The eighth clause, operations security, is of a hybrid nature as well and addresses various issues regarding organizational operations. The human aspect is addressed by elements such as: responsibilities and operational procedures, and audit considerations. The technological aspect is addressed by elements such as: malware, backup, logging and monitoring and control of operational software [5].

The ninth clause, communications security, is mostly aimed at addressing the technological aspects of information security in the form of network controls and information transfer [5].

The tenth clause, system acquisition, development and maintenance, also addresses both these aspects. The aim of this clause is to dictate the security considerations in the development phase of systems and test data [5].

The eleventh clause, supplier relationships, addresses the human aspect of information security. This is done by focusing on information security considerations in supplier agreements and interaction between external systems with that of the organization [5].

The twelfth clause, information security incident management, addresses the human aspect by dictating the responsibilities for the reporting of and responding to information security incidents [5].

The thirteenth clause, information security aspects of business continuity management, is of a hybrid nature. It not only dictates the responsibilities for the integration of information security within the business continuity management system of the organization; but also promotes the implementation of technological controls that ensures the organizational systems are redundant [5].

Finally, compliance focuses (clause 14) on the human aspect of information security by communicating to all relevant parties how compliance will be measured against the organization's ISPA and to ensure legal and statutory requirements are adhered to [5].

All 14 of these clauses not only apply to private organizations, but also directly apply to local government, as they also operate within an environment where information security is a principal issue that needs to be addressed. As mentioned before, these 14 clauses and their controls form the foundation of the contribution in the latter parts of this paper. Thus, this study proposes an architecture and process model that is based on the principles of these very clauses.

Furthermore, as these clauses and the controls within them are central to information security practices, it is beneficial to understand whether the clauses address the human aspect or technological aspect of information security. The benefits of this understanding will be realised when translating various controls into policies for information security, especially when grouping controls of a similar nature together. The manner in which these controls will be utilized in this study will be further discussed later on.

This subsection commenced by introducing basic concepts within information security to provide the needed context for this study. After which the importance and role of policies were discussed in the management process of information security. The focus in the following subsection however, will be to discuss the current state of information security management within local government.

3.2 – South African Local Government and Information Security

As mentioned previously, local government consists of a total of 278 municipalities across three different categories [12]. Every municipality functions as an independent entity, that has to be governed properly in its own right [13]. Consequently, this means that every municipality, although generally working towards the same purpose, will have unique strategic goals, risk appetites, management objectives and operational processes. The implication of this regarding information security is that there is no 'one-size fits all' approach that can be successfully implemented.

In actual fact, a more dynamic approach is needed that caters for the varying administrative and financial capacity of different municipalities. Thus, the Department of Public Service and Administration (DPSA) made a proactive effort towards improving the corporate governance of ICT within government in 2012, which indirectly includes the management of information security. This initiative resulted in the development of the Corporate Governance of ICT Policy Framework (CGICTPF) that aimed to serve as a guiding document for all spheres of government to improve their governance of ICT [14]. In the CGICTPF information security management is advocated as being highly important, however, local government is directed to consult ISO/IEC 27002 and relating documents for further guidance in this regard [14].

This prompted the AGSA to notify local government that its efforts in addressing proper governance of ICT will be measured against the CGICTPF in the following financial year [12]. However, the lack of adequate progress made by local government toward conformance to the CGICTPF led to the AGSA hinting towards a slightly more customised version of the CGICTPF that is being considered, specifically for local government, for the following year [4]. Furthermore, the Department of Local Government in the Western

Cape, informed all municipalities within the province that a new Municipal Corporate Governance of ICT Policy (MCGICTP), that has been adopted by the Department of Co-operative Governance and Traditional Affairs (CoGTA), should be adopted as an agreement has been made with the AGSA with regards to the audit of the 2015/16 financial period [15]. This MCGICTP also places a high importance on information security as it dictates to local government that information security policies should be implemented as part of the first phase of this document [16]. Thus, the ISO/IEC 27002 is a viable source that provides in depth guidance in this regard, as policies are a crucial element advocated by the standard.

Both of these successive initiatives, namely CGICTPF and MCGICTP from government are lacking in detailed guidance for information security management processes. Therefore, it can be argued that local government is in dire need of proper assistance and direction for both the design and implementation of information security management systems.

In this subsection, generally accepted information security management practices were briefly discussed; before discussing the current efforts of local government towards information security. As mentioned above, both the CGICTPF and MCGICTP advocate information security as being highly important, but lack sufficient guidance in this regard. In the following section such an approach will be argued towards that aims to assist local government with the sustainable implementation of information security management.

4. Architecture and Process Model

From the previous section it is evident that the initiatives undertaken by local government, towards information security management are currently unsatisfactory. Therefore, the aim of this section will be to propose both an architecture and process model to assist local government in attaining a higher level of efficacy in implementing information security management. The first part of this contribution will be an architecture, followed by a process model of how the architecture will be implemented.

4.1 – Architecture of Contribution

As mentioned in section 3.1, one of the key elements of information security management is an ISPA. Von Solms and Von Solms assert that policies aim to govern information security and that these policies act similar to organizational laws [11]. These rules and regulations that are dictated by the information security policies of an organization should be uniquely constructed to be relevant for its operating environment. Thus, in creating an ISPA there are several factors that should be considered before attempting to determine its content.

These factors that influence the eventual content of the ISPA, should be formally considered and contemplated throughout this process. There are three central factors that should be considered according to ISO/IEC 27002; namely – risk, legal and organizational objectives and strategic goals. When grouped together, these factors are generally referred to as security requirements as seen in Figure 2 [17].

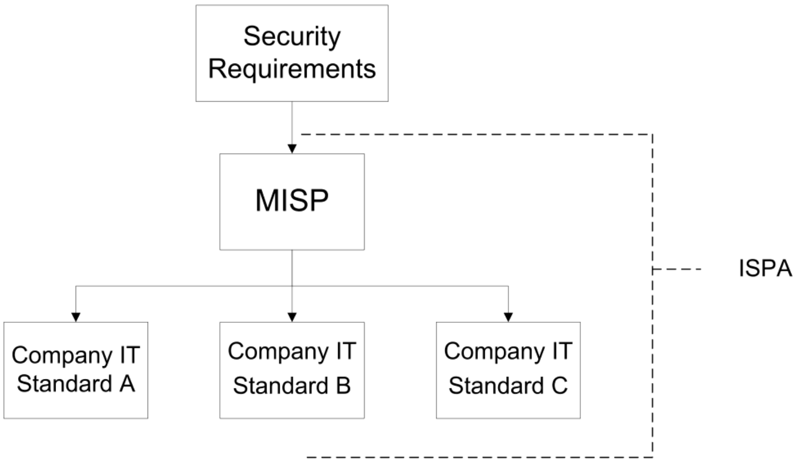


Figure 2 - Information Security Architecture

As depicted in Figure 2, the security requirements provide an input into the high-level municipal information security policy (MISP) and should therefore be considered throughout the process of constructing the MISP. This MISP will dictate: the roles and responsibilities for information security within the municipality, compliance measurement and also provide the reader with a roadmap of the supporting company IT standards and the topics they address within information security. The MISP, as well as the supporting company IT standards, are collectively referred to as the ISPA as depicted in Figure 2.

The supporting company IT standards will provide the necessary details concerning specific issues within information security. These issues will not be addressed at a high level within the MISP; the MISP will merely point to the corresponding company IT standard with a high level statement. As mentioned in section 3.1, these supporting company IT standards will address various issues of a technical and human nature at the level of individual controls. Further details regarding this, will be discussed in the following subsection – where the process model will be introduced.

4.2 – Process Model

In order to ensure that local government are provided with a contribution that is sustainable, a process is needed by which a set of controls can be implemented that is both applicable, and within their financial and administrative constraints. From the semi-structured interviews with local government, it was gathered that it is also imperative that the contribution be dynamic in the sense that every municipality can implement a set of controls that is justified within their specific individual security requirements – consisting of risk, strategic goals and the legal and regulatory requirements.

The dynamic element of the contribution should be of such a nature that every municipality should have a unique set of controls that address their unique needs. The process model depicted in Figure 3, demonstrates the steps of such a dynamic contribution, after which the intricacies of this process are explained.

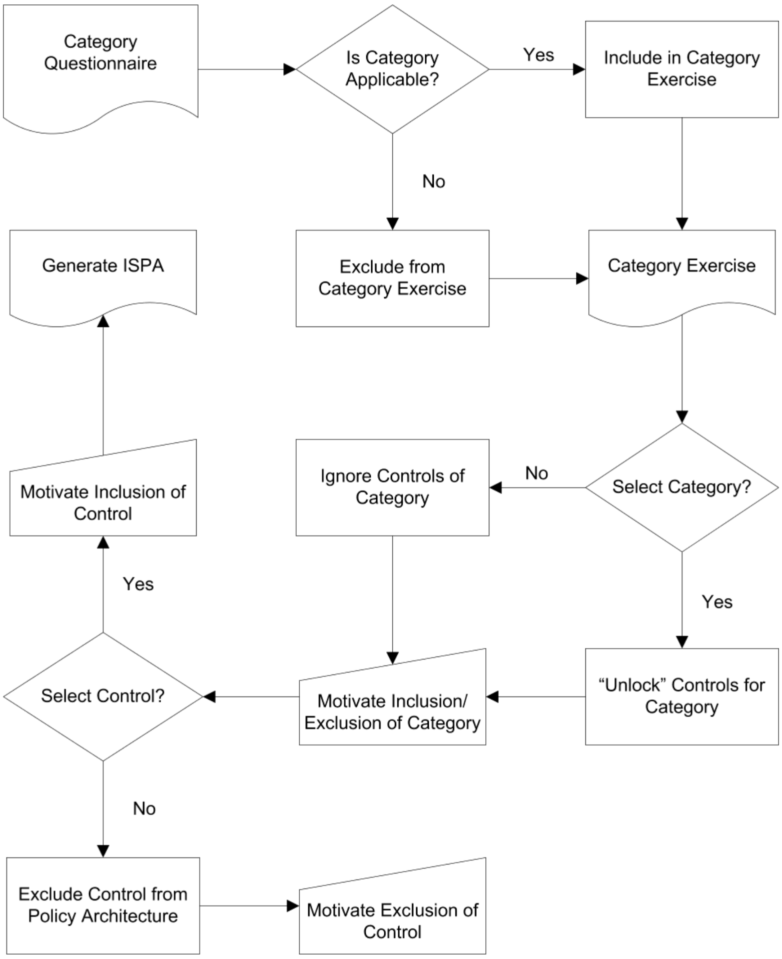

Category Questionnaire
Is Category Applicable?
Yes
Include in Category Exercise
No
Generate ISPA
Exclude from Category Exercise
Category Exercise
Motivate Inclusion of Control
Ignore Controls of Category
No
Select Category?
Yes
Yes
Select Control?
Motivate Inclusion/ Exclusion of Category
"Unlock" Controls for Category
No
Exclude Control from Policy Architecture
Motivate Exclusion of Control

Figure 3 - Process Model for ISPA Development

The goal, and therefore also the envisaged output, of the entire process model is to follow a process to develop a unique ISPA for different municipalities that address their individual security requirements. In order to achieve this, as seen in Figure 3, a questionnaire will first of all be used to determine whether or not there are any categories within ISO/IEC 27002 that are not applicable to local government due to their unique operating environment. This will be accomplished by engaging in further semi-structured interviews with local government officials.

Once this is established, the categories that are applicable will be presented to local government for consideration in spreadsheet-based electronically automated exercise. In this exercise, local government will decide whether or not a security category is applicable to them individually, based on the category's objective – while also considering their financial and administrative capacity. As depicted in Figure 3, based on their choice for each category, justification has to be provided for either, inclusion to - or exclusion from, the remainder of the exercise before progress can be made.

Subsequently, the controls for each category that has been chosen for inclusion will be listed with further details and objectives of the control for local government to consider – while the controls for excluded categories will be excluded from the ISPA. Again, the inclusion or exclusion of every control from the ISPA will have to be justified. Upon completion of this exercise, an ISPA will be generated - derived from the controls that were selected for inclusion by the municipality.

Thus, the final set of controls that remain will be applicable and will be translated into a MISP and supporting company IT standards. The following section will reflect on the achievement of the objectives of this paper.

5. Conclusion

This paper argued that ICT has become absolutely critical to the success of the modern day organization, so much so that the very survival of the organization almost depends on the efficacy of its ICT function. This can be attributed to the fact that most, if not all business functions are almost completely dependent on it. It was further argued that the information, that is processed, stored and transported by these ICT systems, needs to be protected. Local government are no different, in that ICT plays a crucial role in achieving their goal of serving their communities. However, even though information security is of paramount concern, local government is struggling to attain effective information security management.

The objective of this paper was therefore; to propose a process by which local government can improve their information security management. This objective was met by introducing the reader to the architecture and process model, advocated by this research. The architecture depicts the envisaged output or artefact that will stem from the bigger research project. While the process model, illustrates the steps that will be followed in the development of the ISPA. This process aims to establish an applicable set of controls for each municipality that follows this process. In turn, this will enable the local government of South Africa, and similarly also the rest of Africa, to more effectively manage information security practices. Consequently, better information security management leads to the improvement of the general ICT function within local government, which enables them to deliver services to their communities in a sustainable manner.

Further research is being done in this regard, by working towards the development of a prototype of this process. The prototype will be in the form of an exercise that will be completed as a workshop with local government officials to verify its validity. These results will be published at a later stage.

Acknowledgments

The financial assistance of the Nelson Mandela Metropolitan University (NMMU) for this research is hereby acknowledged. Opinions expressed and conclusions argued towards in this paper are those of the authors and are not necessarily to be attributed to the NMMU.

References

[1] M. Whitman and H. Mattord, “Principles of Information Security: Thompson Course Technology,” *Kennesaw State Univ.*, 2003.

[2] M. Gerber, R. Solms, and P. Overbeek, “Formalizing information security requirements,” *Inf. Manag. Comput. Secur.*, vol. 9, no. 1, 2001.

[3] Republic of South Africa, “Constitution of the Republic of South Africa, 1996 - Chapter 2: Bill of Rights.” .

[4] Auditor-General of South Africa (AGSA), “The status of controls: Be well governed and demonstrate good governance and administration,” 2013.

[5] Iso/Iec 27002, *Information technology — Security techniques — Code of practice for information security controls*. 2013.

[6] 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.

[7] Pacific Research and Evaluation Associates, “Semi-structured Interview,” 2010. [Online]. Available: http://evaluationtoolbox.net.au/index.php?option=com_content&view=article&id=31&Itemid=137. [Accessed: 01-Dec-2015].

[8] Iso/Iec 27000, “Information technology — Security techniques — Information security management systems — Overview and vocabulary,” 2012.

[9] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, “Information security conscious care behaviour formation in organizations,” *Comput. Secur.*, vol. 53, pp. 65–78, 2015.

[10] S. Furnell and N. Clarke, “Power to the people? the evolving recognition of human aspects of security,” *Comput. Secur.*, vol. 31, no. 8, pp. 983–988, 2012.

[11] R. Von Solms and B. Von Solms, “From policies to culture,” *Comput. Secur.*, vol. 23, pp. 275–279, 2004.

[12] Auditor-General of South Africa (AGSA), “Consolidated general report 2012/13,” 2012.

[13] Local Government, “Municipal Systems Act,” vol. 32, 2000.

[14] DPSA, “Public Service Corporate Governance of Information and Communication Technology Policy Framework,” no. December, 2012.

[15] Western Cape: Department of Local Government, “Local Government Circular: C5 of 2015.” 2015.

[16] (CoGTA) Department of Co-operative Governance and Traditional Affairs, W. C. D. of L. Government, and (SALGA) South African Local Government Association, “Municipal Corporate Governance of Information and Communication Technology Policy,” no. January, pp. 1–19, 2015.

[17] M. Gerber and R. von Solms, “From Risk Analysis to Security Requirements,” *Comput. Secur.*, vol. 20, pp. 577–584, 2001.

Appendix E - Journal of Public Administration (Under Review)

The journal paper titled ***'A Self-Help Approach to Information Security Management in Local Government'****, has been submitted to the South African Journal of Public Administration in 2016. This paper was written to showcase the complete study and is currently in the review process.*

A Self-Help Approach to Information Security Management in Local Government

ABSTRACT: ICT is a crucial function in any modern organization. This has led to increasingly more organizations putting their best efforts into protecting their information and information-processing systems via the process of information security management. Local government is faced with similar challenges when implementing information security management as those of any other organization. However, their attempts at implementing information security management generally remain unsatisfactory. Therefore, the aim of this paper is to address the shortcomings of local government, and to provide them with a self-help approach to information security management. This approach was developed by using mixed methods throughout various cycles of refinement within a local government context.

1. Introduction

Most core business functions within the modern organization rely heavily on Information and Communication Technology (ICT) systems to successfully fulfil their role in the organization (Ifinedo, 2014). This undeniable dependency on ICT places a big responsibility on the ICT function of an organization to perform at an optimal level, consistently. The responsibility that rests upon the ICT function is further heightened by the multitude of risks that threaten the safety of all informational assets, and related ICT systems, within the organization. In order to successfully mitigate these risks, they need to be addressed by the process of information security management.

Generally, when attempting to implement sound management of information security, the focus is mostly on protecting the confidentiality, integrity and availability of information – commonly referred to as the CIA of information (Mariana Gerber, Solms, & Overbeek, 2001). In ensuring the protection of these three properties (CIA), two main factors are prominently targeted in practice. The first is the use of various technological controls – in an attempt to ensure that the CIA of the information remains intact against – mostly – external threats (Sohrabi Safa, Von Solms, & Furnell, 2016). The second factor is the socio-organizational context, where the focus is more on the human aspect involved with information security, for instance – protecting the information from internal threats largely – like negligent or ignorant employees (Furnell & Clarke, 2012; Sohrabi Safa et al., 2015).

These two factors of information security are equally important for the success of any information security program (Ifinedo, 2014). The importance of addressing information security at an executive level is undeniably a growing concern. Thus, the above-mentioned applies to organizations across both private and public sectors. Consequently, this also applies to the whole sphere of local government within South Africa.

Local government within South Africa consists of 278 municipalities, of which each individual municipality operates as a fully functional independent entity that serves its local community. All these municipalities are externally audited by the Auditor-General of South Africa (AGSA) on various control areas each year – of which information technology is one. The findings of these audits are published in the form of a formal audit report. Furthermore, the AGSA advocates that four key risk areas within ICT need to be addressed by local government (AGSA, 2013). One of those four key risk areas is information security management, and the urgency with which it should be addressed by local government is continually stressed by the AGSA annually; as is evident in the latest report of 2013/14 (AGSA, 2013).

In the latest audit report, of the 2013/14 financial period (AGSA, 2013), more than half of all municipalities are facing challenges with either the design, or the implementation of effective controls for information security management, as may be seen in Figure 1. Although this percentage is a slight improvement on that of the previous year, the progress is slow. This slow progress still leaves local government in a vulnerable position in terms of information security. In the light of the above-mentioned, it should be very clear that the problem addressed by this paper is specific to local

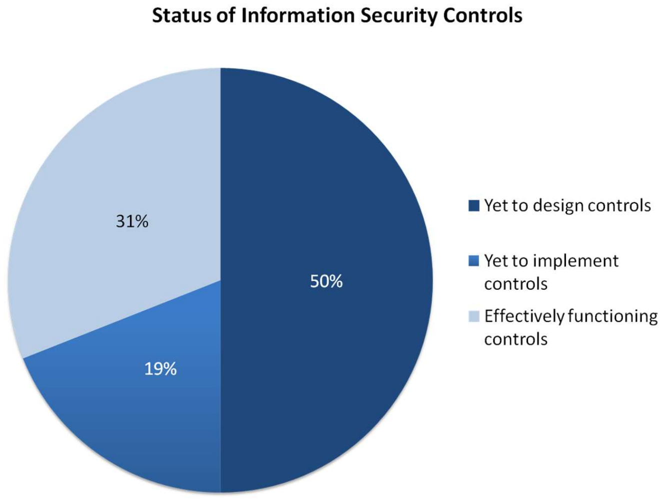


Figure 1 - Findings on information security controls (AGSA, 2015)

government's unique operating environment and to the related difficulties with implementing successful information security management structures.

The aim of this paper is to provide insight into the situation within local government, in terms of information security management, and to provide local government with the necessary tools and skills to empower them to help themselves in achieving effective information security management. However, although information security management is a very broad and multifaceted concept, this paper mainly focuses on the policy-related aspects of information security management. This paper will discuss the research approach followed for this study, before elaborating further on the information security landscape within local government. Following this, the various information security management approaches will be mapped, according to the relevant principles that are vital in any successful contribution to local government. The principles will then be used as criteria for the proposed contribution. This contribution was validated against these principles; and it will be reported on.

2. Research Approach Followed

The research approach followed in this study is design-oriented in nature, whereby the researchers aim to produce or develop an artefact as an answer, or as a solution, to a real problem in industry (Österle et al., 2011). The research was also conducted in a cyclical nature, whereby engagement with practitioners was used to refine the artefact through as many cycles as were necessary, until both the researchers and the practitioners were satisfied with the artefact.

The cycles of refinement were accomplished by engaging in semi-structured interviews with local government officials that work within the ICT function of their municipality. A single District Municipality in the Western Cape was chosen for this study, because of the clean audit result of their ICT function in the latest audit report of the AGSA. These semi-structured interviews created the opportunity for the researchers to present propositions to five local government officials, representing the whole ICT function, as well as one representative from a business/risk function. It was also possible to engage in discussions afterwards, in order to gain feedback. This feedback was then documented and used to change, adapt and improve the contribution accordingly. The improved contribution was then again subject to discussion in further cycles of semi-structured interviews with the same local government officials within the ICT function of the above-mentioned District Municipality.

The initial draft of the contribution was based solely on literature work and international standards. However, all the subsequent versions of the contributions were adapted, according to the feedback from the semi-structured interviews, leading finally to the contribution in its current state, as presented in this paper. This approach ensured firstly, that the foundation of the artefact had a sound theoretical basis – by drawing from the literature and international standards. Secondly, it also allowed the artefact to be dynamic, in the sense that it addresses the unique and specific challenges faced by local government, by engaging directly with practitioners in this sector. This contribution was validated by means of a workshop that was attended by 20 municipal representatives from the various municipalities across the Eastern Cape.

3. Information Security Management in Local Government

It is argued that information security management is critical in local government. This section aims to elaborate on the current efforts of local government in the implementation of information security management; and it will explore the traditional approaches to information security management, in order to provide a theoretical basis for the proposed contribution of this paper. Finally, the principles derived from the unique operating environment and the challenges of local government, to which the proposed contribution has adhered, will be argued.

3.1. Status of Information Security Efforts of Local Government

As previously mentioned, local government is audited annually by the AGSA. The aim of this audit is not only to measure performance, but ultimately to improve performance within local government – by making recommendations for remedial action (AGSA, 2013). Furthermore, the AGSA regularly engages with local government to provide additional assistance and guidance with regard to the various challenges with which they are faced. Within ICT, in particular, the aforementioned engagement is evident in the fact that the AGSA collaborated with the Department of Public Service and Administration (DPSA) and the South African Local Government Association (SALGA) in 2012 – to develop a Corporate Governance of ICT Policy Framework (CGICTPF).

This CGICTPF was developed in an attempt to address the various challenges regarding the adequate use and governance of ICT within the South African government: nationally, provincially and locally. The biggest of these challenges in question was found to be, firstly, a lack of involvement; and secondly, the limited support from top management. These issues are both very crucial in ensuring the proper governance of ICT (DPSA, 2012). The lack of these two factors is in direct contradiction of what the Presidential Review Commission (PRC) report of 1998 advocated; since ICT should be governed properly with decision-making flowing from senior political and managerial leadership (DPSA, 2012). Although the PRC report had already advocated this towards the end of the 20th century, the AGSA reiterated more than a decade later in the audits of both the 2008/09 and 2009/10 financial periods, the need for a framework that would enable the proper governance of ICT in local government. And consequently, the CGICTPF was developed, as the AGSA collaborated with the DPSA and the SALGA.

The CGICTPF is to a large extent based on the ISO/IEC 38500 international standard and other best practices, such as COBIT 5 and the King III Report on Governance (DPSA, 2012). According to the CGICTPF, information security is one of the topics within ICT that should be addressed by executive management (DPSA, 2012). However, the focus of the CGICTPF is on the corporate governance of ICT; and thus, it does not provide detailed guidance in terms of information security management.

Implementing information security management practices by adopting or consulting the ISO/IEC 27000 set of standards is recommended by the CGICTPF as a bare minimum (DPSA, 2012). However, the ISO/IEC 27000 set of standards are not the only standards or best practices that provide guidance for information security practices. The importance of information security management within the corporate governance of ICT is also supported by best practices, such as COBIT 5 and the King III Report on Governance. Within COBIT 5, this is evident as one of the 'Processes for the Governance of Enterprise IT' is managing security. In the King III Report on Governance, a whole chapter is dedicated to the governance of ICT; and within it there are 7 principles that are recommended, one of which also focuses largely on the management of information security.

Considering the above-mentioned and the fact that the CGICTPF is applicable to all spheres of South African government, an issue with regard to scalability becomes evident in the local government sphere. This is due to their limited financial and administrative capacity, which pales in comparison with the amount of resources at the disposal of the provincial and national spheres of government. Consequently, this has led to further development of an approach to corporate governance of ICT that is more specific to the unique needs and the limited capacity of local government in response to a directive from the minister of Co-operative Governance and Traditional Affairs (AGSA, 2013).

The aforementioned approach is called the Municipal Corporate Governance of ICT Policy (MCGICTP); and it was developed collectively by the Western Cape Department of Local

Government, Department of Co-operative Governance and Traditional Affairs, the DPSA, SALGA and the Western Cape Provincial Treasury.

Within the MCGICTP, as with the CGICTPF, the responsibility for information security management is placed with executive management. In order to address it, however, the MCGICTP recommends the creation of various policies in this regard, without giving any additional guidance. Furthermore, the acknowledgement of the scalability issue in the local government context that led to the development of the MCGICTP is supported by internal correspondence within the Department of Local Government of the Western Cape. This is evident; since it is stated in the '*Local Government Circular: C5 of 2015*' that "the CGICTPF referred to Municipalities by the DPSA was too complex to implement in Municipalities; as it did not consider the unique operating environments within Municipalities" (Western Cape: Department of Local Government, 2015).

Although the MCGICTP is said to have been adapted for local government, it remains largely similar to the CGICTPF. As in the case of the CGICTPF, the MCGICTP only addresses 'WHAT' needs to be done; and it does not provide any detailed guidance on 'HOW' it must be done. The WHAT-factor, in both the CGICTPF and the MCGICTP, as stated before, stems from international standards and best practices. However, these generally strive towards a perfect-world scenario. This is unattainable in local government because of the limited financial and administrative capacity at their disposal. Thus, any proposed contribution that aims to assist local government with the implementation of information security management must strive to overcome this challenge, and should effectively address the 'HOW'.

3.2. Traditional Approaches to Information Security Management

Information security is typically addressed by implementing a relevant set of controls, both technological and socio-organizational in nature (Da Veiga, Martins, & Eloff, 2007; Ifinedo, 2014; Sohrabi Safa et al., 2015, 2016). Furthermore, it is generally accepted that the main objective of such a set of controls is to protect or ensure the confidentiality, integrity and availability of information by mitigating risks that threaten these three aspects (ISO/IEC 27002, 2013). It should be noted at this point that the ISO/IEC 27002, and the controls it recommends, will form the theoretical base of the contribution to be proposed in section 4. However, before a relevant set of controls can be obtained by an organization, the specific information security requirements of the organization should be clearly stipulated (Gerber, Von Solms, & Overbeek, 2001; Gerber et al., 2001).

There are various processes and considerations that should feed into the effective formulation of information security requirements. These include as a bare minimum: a risk assessment exercise to determine the risk requirements, as well as the legal and regulatory requirements within the operating environment of the organization, together with the objectives and requirements of business for ICT to support business functions (ISO/IEC 27002, 2013). In essence, the security requirements should address the information security risk environment of the organization, in such a way that they align with and support the business objectives of the organization, while also taking into consideration the legal, regulatory and contractual requirements that should be satisfied.

When information security requirements have been identified and clearly stipulated, a suitable and unique set of controls that addresses the security risk profile of the organization can be identified and implemented (Gerber & von Solms, 2008; ISO/IEC 27002, 2013). Ultimately, this set of controls will represent the direction that the organization wants to move in, with regard to information security. These said directives for information security should ideally be communicated in various policies (Von Solms & Von Solms, 2004). Furthermore, these policies should be driven by strategic management – right down to the operational level. And, they should dictate the appropriate behaviour of employees in terms of information security (Von Solms & Von Solms, 2004).

Typically, the information security policies and the related documents of an organization are structured in the following manner: a high-level policy that provides management direction and drive for the rest of the information security programme; this must be supported by several sub-policies, company standards, guidelines and processes that are usually issue or topic-specific; and they provide more detailed guidance in this regard (ISO/IEC 27002, 2013; Von Solms & Von Solms, 2004). This structure or hierarchy of policies, company standards and related documents is usually collectively called an information security policy architecture (ISPA).

However, having an ISPA alone does not completely solve the issue of information security; as there are many more considerations in the human aspect of security that need to be addressed (Furnell & Clarke, 2012; Sohrabi Safa et al., 2015). These additional aspects of information security that fall beyond the influence of policies *per se*, are addressed however by the overarching information security management system (ISMS). According to the ISO/IEC 27000 standard, an ISMS is defined as comprising “the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets” (ISO/IEC 27000, 2012). Thus, by implementing an ISMS, this enables an organization to holistically address the information security concerns; since it goes beyond merely dictating a set of controls in an ISPA, to also include the management of additional resources and activities, to further ensure the safety of its information assets.

Considering that all the above-mentioned – which is essentially 'WHAT' should be done to successfully implement information security management – it is quite clear and straightforward that local government still needs guidance in addressing the 'HOW' it should be done in the face of the various constraints and challenges that are unique to the operating environment. The following subsection will thus argue towards those principles that should be incorporated into the contribution that addresses these challenges that are specific to local government.

3.3. Information Security Management Principles for Local Government

As mentioned before, the operating environment of local government is very unique; and it is fraught with challenges that inhibit any attempts towards a perfect-world implementation of any solution. Therefore, the contribution proposed by this paper will extend beyond the 'WHAT' that was discussed in the previous subsection; since it is also based on several additional principles. These principles will aim to further improve the applicability of the contribution to local government's situation and to better address some of their challenges.

Firstly, the contribution should be *SCALABLE* to address the varying resource capacity of different municipalities. SALGA states that "municipalities operate in a very isolated and non-uniform manner" (SALGA, 2012). This further motivates the need for a contribution that scales really well, because of the non-uniformity across local government. The scalability of the contribution should also enable municipalities to implement information security – in spite of their financial constraints.

Secondly, the contribution should be *SIMPLISTIC* – so that it is not complex, but rather easy to understand. The simplicity of the contribution will aim to empower employees that do not necessarily have adequate skills, to also be able to contribute towards implementing information security. Regarding the afore-mentioned, SALGA breaks the harsh reality that "the staff is made up of under-qualified professionals with watered-down skills that are not geared for real-life ICT crises and challenges" (SALGA, 2012). In addition to having a skills shortage, financial constraints often render low capacity municipalities even more vulnerable; because they cannot afford to involve external consultants.

Thirdly, the contribution should be *USABLE,* so that it can be readily implemented in a real-world environment straightaway. As mentioned in section 2 of this paper, this research aims to provide a practical contribution to this very real problem in local government. Therefore, the contribution must be of such a nature that it can be readily implemented – without having to be adapted or improved on by local government – before they can use it.

Lastly, the contribution should be *HOLISTIC*; so that it addresses the topic of information security and its management comprehensively. To ensure that information security practices are covered comprehensively, established best practices and international standards will be drawn from, in order to form the basis of the contribution.

The contribution that will be presented in the following section will aim to incorporate the above-mentioned principles.

4. A Self-Help Approach to Information Security Management in Local Government

As mentioned before, local government is constantly faced with administrative and financial constraints. Therefore, the contribution proposed in this section will aim to provide local government with a self-help approach that largely negates the aforementioned challenges of limited resources, both financially and in terms of skilled personnel. This contribution has two parts, of which the first is an architecture; and this is followed by a process that illustrates the proposed steps required to develop an ISPA.

4.1 Architecture for Information Security Management in Local Government

The architecture proposed in this subsection provides most of the WHAT-factor for municipalities in terms of artefacts that need to be in place, in order to effectively manage information security. The content of these artefacts is in line with international standards and best practices, as described in section 3.2 and Figure 2.

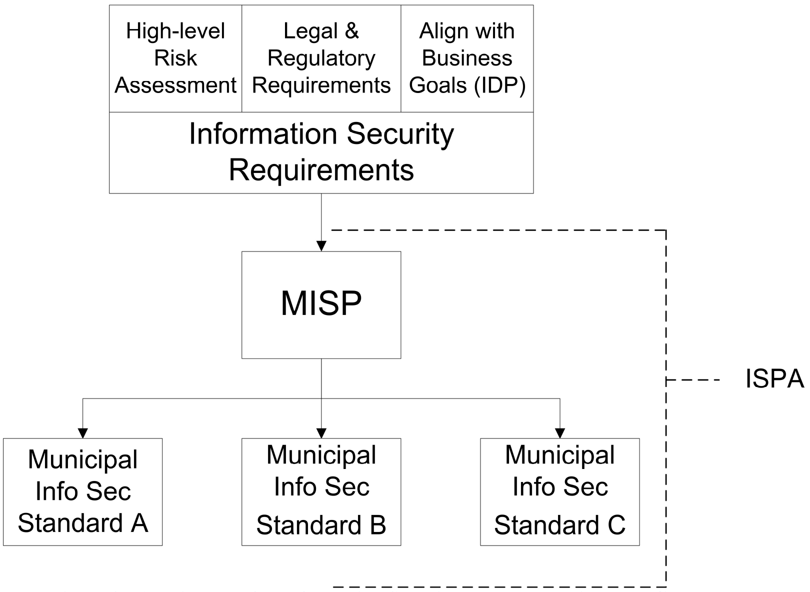

High-level Risk Assessment
Legal & Regulatory Requirements
Align with Business Goals (IDP)
Information Security Requirements
MISP
ISPA
Municipal Info Sec Standard A
Municipal Info Sec Standard B
Municipal Info Sec Standard C

Figure 2 - Architecture for Information Security Management in Local Government

The *Information Security Requirements* should be based on the results of a high-level risk assessment; they should align information security with strategic business goals, which is the IDP in the case of municipalities, as well as giving consideration to the legal and regulatory environment in which the municipality operates.

The *MISP* serves the role of a high-level information security policy that communicates the directives of executive management for information security to all the employees. The organization of information security, as well as the roles and responsibilities for information security, will also be contained in this document. Due to the high-level nature of this document, it will be constructed in a non-technical manner without giving guidance for specific processes at the operational level.

The various *Municipal Information Security Standards* that stem from the *MISP* will provide this more technical and detailed guidance for information security practices. Each of the *Municipal*

Information Security Standards will address the specific interrelated issues, which can be logically grouped together under one topic, for instance *User Access Management*, *Internet & E-mail Usage* or *Network Security*. Although Figure 2 depicts only three such standards, the proposed contribution is not limited to only three supporting standards. These three standards are purely an example for the purpose of showing the hierarchy of the *ISPA*.

The *ISPA* consists of the collection of the *MISP* and the *Municipal Information Security Standards* that support it. The *ISPA* of a municipality, that is unique and specific to their *Information Security Requirements*, which will be generated in an automated manner upon completion of the process; and this will be discussed in the following subsection.

4.2 Process for Information Security Management in Local Government

It is important to note, as mentioned in section 3.2, that the ISO/IEC 27002 standard forms the theoretical basis of the contribution. Furthermore, as stated previously, the purpose of the process that will be discussed in this subsection is to guide municipalities through a series of steps, with the final goal of generating an *ISPA* that addresses their *Security Requirements*. The process depicts the mechanical working of the exercise that will be presented to municipalities in a spreadsheet format.

This *Process for Information Security Management in Local Government* has three steps that are depicted in Figures 3, 4 & 5, respectively. The first step in the *Process* focuses on the categories within ISO/IEC 27002.

As depicted in Figure 3, a municipality will be presented with the categories of ISO/IEC 27002,

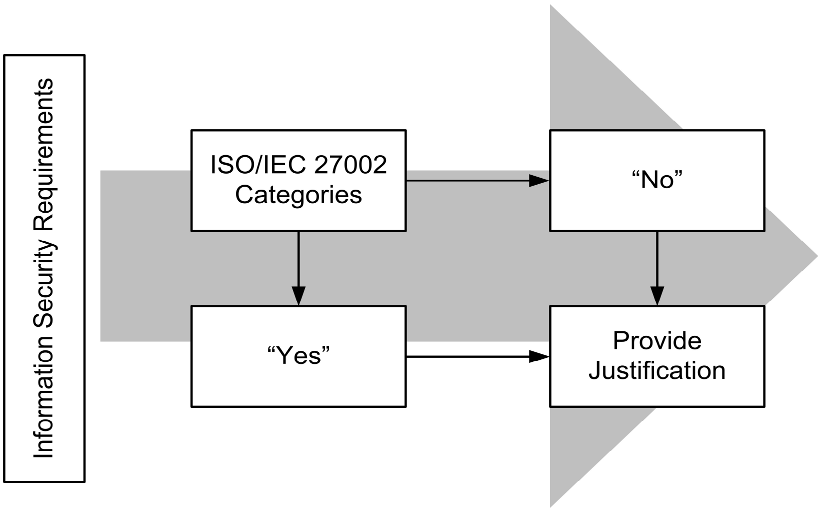


Figure 3 - Process for Information Security Management in Local Government - Category Selection (Step 1)

along with the objectives of these categories, for consideration. Based on the explanation of the objective of the category, the municipality must decide whether or not these apply to them. However, throughout this first step of the *Process*, the selection of categories should be based on the *Information Security Requirements*. Furthermore, the municipality must *Provide Justification* for every selection they make, both when they select and reject a category.

Upon completion of this step of the *Process*, the categories that were declined by the municipality will be ignored and excluded from the remainder of the *Process*. However, those categories that were selected by the municipality will be further elaborated upon; as all the controls within those categories will be presented for consideration. This is depicted in Figure 4.

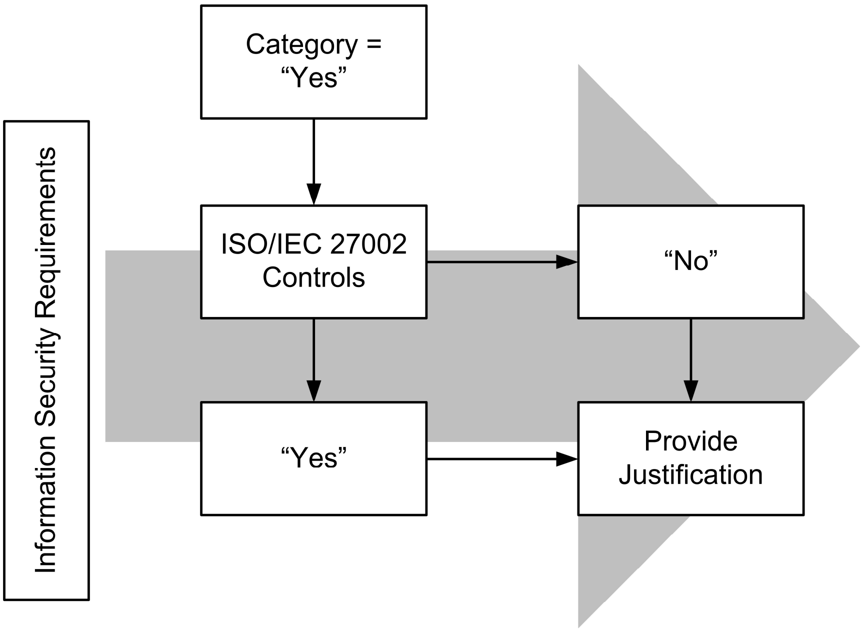


Figure 4 - Process for Information Security Management in Local Government - Control Selection (Step 2)

Again, similar to the previous step of the *Process*, controls will be presented to municipalities for consideration, along with the objectives of the controls. The difference, however, is that for every one category there are multiple controls to consider. The selection of every individual control, as depicted in Figure 4, should be influenced by the *Information Security Requirements*. Furthermore, as before, a municipality should *Provide Justification* for both, the selection and the rejection of a control. At the end of this step in the *Process*, a municipality will have a set of controls that are applicable to them, and which they should be able to implement from a resource-and-capacity perspective.

The final step of the *Process*, as depicted in Figure 5, is based on the selection of controls by the municipality. The set of controls will be translated into an *ISPA* that will be applicable; as it is based on the specific *Security Requirements* of the municipality.

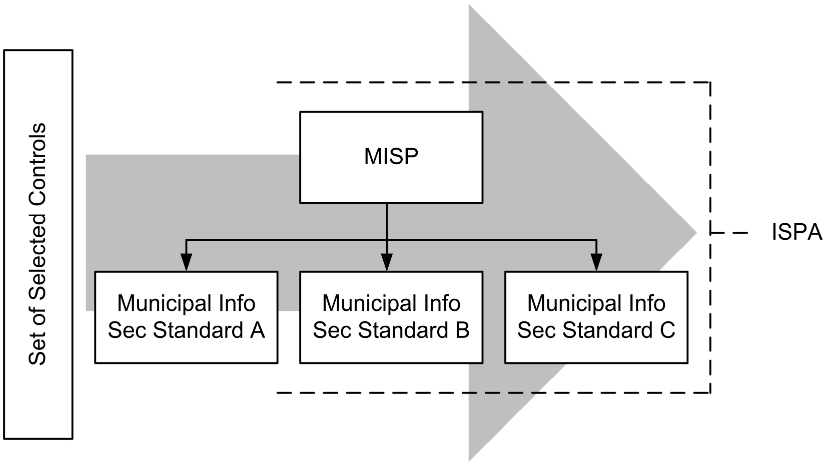

Set of Selected Controls
MISP
Municipal Info Sec Standard A
Municipal Info Sec Standard B
Municipal Info Sec Standard C
ISPA

Figure 5 - Process for Information Security Management in Local Government - ISPA Generation (Step 3)

The translation from controls into the *ISPA* will be an automated step in the *Process*, which is built into the spreadsheet-based presentation of the contribution. The selected controls will be integrated into and communicated via the ISPA, from the high-level *MISP* right through to the *Municipal Information Security Standards,* with the relevant details and technicality, respectively.

4.3 Addressing the Principles and Challenges of Information Security Management within Local Government

As previously stated, this contribution aims to adhere to four principles that ensure that the contribution addresses the unique challenges of local government. Of the aforementioned challenges, a lack in skills and resources is one of the most prominent; and it calls for a contribution to be *SCALABLE*. Thus, any municipality should be able to use the proposed contribution, regardless of their financial and administrative capacity. The proposed contribution incorporates this principle –

by requiring municipalities to choose their own specific set of controls, which are attainable by them, as opposed to prescribing them with a static set of controls that might lead them into a position where they proverbially “bite off more than they can chew”.

Another challenge that is prominent in the local government context is that the staff are generally under qualified; and they do not possess the required skills. This challenge calls for the proposed contribution to be *SIMPLISTIC*; so that it can be completed by employees, regardless of their information security knowledge or skills prior to implementation. The contribution addresses this challenge by proposing a simple and easy-to-follow process, while also providing the objectives of categories and controls; so that it is more comprehendible to such individuals.

Furthermore, the proposed contribution is constructed in a practical manner to be *USABLE* in a real-world scenario. The need for this principle, as mentioned before, is due to the practical nature of the problem addressed by this research.

Finally, the researchers aimed to provide a *HOLISTIC* approach to information security management. This principle ensures that local government have a contribution that addresses information security, in line with what the norm is in industry across all sectors, by drawing from international standards and best practices.

5. Validation of Contribution

The contribution described in the previous section, as mentioned before, aims to meet four additional principles, above and beyond that of contemporary information security management practices. This adaptation and specifically tailored approach to information security management is focused on addressing challenges that are largely unique to the local government operating environment. In order for the researchers to measure to what extent the contribution meets these additional principles of *SCALABLE, SIMPLISTIC, USABLE* and *HOLISTIC,* a validation exercise was undertaken in the form of a workshop of the contribution.

The workshop was conducted with 20 participants, representing different municipalities across the Eastern Cape. The majority of the participants work within the ICT; and they function within their respective municipalities, with some representatives from the financial and/or business oriented capacity. All of the participants attended the same two-day workshop; and they were presented with a practical representation of the contribution in a spreadsheet-based format.

This spreadsheet-based tool was explained by the researchers in a 2-hour long session. The tool was however not only explained, but was also interacted with the participants in a practical engagement, upon which they could ask questions and run through various exercises to test the functionality of the tool. In order for the researchers to gain insight into how the participants perceived this tool, as well as whether or not, the principles were satisfied by the tool, the participants were handed a questionnaire at the end of the workshop session to gather these data.

Upon analysing the data collected from the questionnaires, it was found that the majority of the participants agreed that the practical representation of the contribution, a spreadsheet-based tool, incorporated all four principles. A consolidated 95% of the participants agreed that the contribution was both *HOLISTIC* and *SCALABLE.* With regard to questions testing for the contribution being *USABLE*, all the participants agreed unanimously that this principle was present in the tool. The participants, when asked about the contribution being *SIMPLISTIC*, answered a little less favourably than they had done with the other principles; however, 72.5% still agreed that this principle was being met.

Therefore, it is reasonable to argue that the contribution of this paper did indeed incorporate the four principles of *SCALABLE, SIMPLISTIC, HOLISTIC* and *USABLE.* Again, it is important to note that these principles are aimed at addressing challenges that are specific to the local government context. Thus, it is also reasonable, based on the above-mentioned evidence, that the contribution addresses the unique challenges of local government; because it incorporates the above-mentioned principles.

6. Conclusion

The critical nature and the need for, information security in modern-day organizations cannot be denied. This fact holds true, regardless of the geographical location, or the type of organization in question. Therefore, information security should necessarily also be managed properly by local government in South Africa. The Auditor-General of South Africa audits local government annually on various control areas, of which ICT is one. Within ICT, these audits reflect that information security management efforts within local government are unsatisfactory; and this is a matter of grave concern.

The contribution proposed in this paper consists of two parts, the first being an "*Architecture for Information Security in Local Government",* which is accompanied and supported by the second part, a "*Process for Information Security Management in Local Government"*. The collective contribution incorporates four principles, in order to address the unique challenges that are specific to local government, by ensuring that the contribution is *SCALABLE*, *SIMPLISTIC*, *USABLE* and *HOLISTIC*. This was validated in the workshop described in the previous section.

7. References

Auditor-General of South Africa (AGSA). (2013). *The status of controls: Be well governed and demonstrate good governance and administration*.

Da Veiga, A., Martins, N. & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *South African Business Review*, *11*(1).

DPSA. (2012). Corporate Governance of Information and Communication Technology Policy Framework, (December).

Furnell, S. & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988.

Gerber, M., Solms, R. & Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security*, *9*(1).

Gerber, M. & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5-6), 124–135.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79.

ISO/IEC 27000. (2012). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27002. (2013). *Information technology — Security techniques — Code of practice for information security controls*.

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–

SALGA. (2012). A Municipal Guide / Roadmap To Successful ICT Governance, (June), 93.

Sohrabi Safa, N., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.

Sohrabi Safa, N., von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13.

Von Solms, R. & Von Solms, B. (2004). From policies to culture. *Computers and Security*, *23*(4), 275–279.

Western Cape: Department of Local Government. (2015). Local Government Circular: C5 of 2015.

LoveToEdit

You Write. We Edit. You Love it.

03 December 2016

TO WHOM IT MAY CONCERN

REF: CONFIRMATION OF LANGUAGE EDITING SERVICES: JOSHUA DE LANGE

I confirm that I have done Language Editing for Joshua de Lange's Dissertation titled:

A FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT IN LOCAL GOVERNMENT.

The Dissertation now conforms to Nelson Mandela Metropolitan University's language editing standards.

Yours sincerely

Sibanda

Lynn N Sibanda

Tel: 011 050 0376

Mobile: 071 989 0983

Email: lynn@lovetoedit.co.za

Member of the Professional Editors Guild

Professional
EDITORS
Guild

Psalm 29:1-2

1Give unto the Lord, O ye mighty, give unto the Lord glory and strength.

2Give unto the Lord the glory due unto his name; worship the Lord in the beauty of holiness.

Habakkuk 2:14

14For the earth shall be filled with the knowledge of the glory of the Lord, as the waters cover the sea.