

**A MODEL FOR THE ALIGNMENT OF  
INFORMATION SECURITY  
REQUIREMENTS WITHIN SOUTH  
AFRICAN SMALL, MEDIUM AND MICRO  
ENTERPRISES**

by

**Timothy H. Speckman**



**A MODEL FOR THE ALIGNMENT OF  
INFORMATION SECURITY  
REQUIREMENTS WITHIN SOUTH  
AFRICAN SMALL, MEDIUM AND MICRO  
ENTERPRISES**

by

**Timothy H. Speckman**

**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. Mariana Gerber**

April 2019



# Declaration

I, Timothy H. Speckman, hereby declare that:

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

A handwritten signature in black ink, consisting of a large, stylized 'T' and 'S' intertwined, with a horizontal line crossing through the middle.

---

Timothy H. Speckman

# Abstract

Small, medium and micro enterprises (SMMEs) are reported to be the hope of the economy in many developing countries, such as South Africa (SA). The unique characteristics of SMMEs such as their ability to evolve rapidly, and to employ larger labour forces as they grow, make these enterprises valuable to the SA economy, in which poverty and unemployment rates are alarmingly high. Like most modern enterprises, SA SMMEs make use of information and communication technology (ICT) systems - as a vehicle to store, transmit and process information, which is an asset that is critical to their business operations. Thus, the vulnerabilities of these ICT systems need to be addressed, in order to protect the information assets of enterprises. However, SMMEs are known to only implement measures to protect their information assets on an ad hoc basis and frequently as reactive measures to information security incidents.

This can be attributed to the fact that most of these enterprises lack the ability to establish their unique information security requirements. Information security requirements are a measure of the level of security needed to adequately protect the information assets of an enterprise. Furthermore, it is reported that information security best practices and standards, which provide guidance on information security, are too complex for SA SMMEs to implement and for SMMEs to use for establishing their unique information security requirements.

Therefore, this dissertation reports on research that was conducted to develop a model to simplify the manner in which SA SMMEs can determine their information security requirements. To accommodate the characteristics and challenges of SA

SMMEs, this model seeks to be both scaleable and simplistic enough to implement across all categories (small, medium and micro) of SA SMMEs .

# Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Prof. Mariana Gerber for her continuous support during my Master's study. Furthermore, I would like to express my gratitude for her patience, motivation, enthusiasm, and immense knowledge. Her guidance assisted me throughout the research and the writing of this dissertation. I could not have imagined having a better supervisor for my Master's study.

A special thank you goes to Dr Patrick Goldstone , who corrected all my spelling, grammatical and typographical errors.

Furthermore, 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 they not necessarily to be attributed to the National Research Foundation.
- The financial assistance of the Nelson Mandela University's Post Graduate Research Scholarship (PGRS) is also hereby acknowledged.

Not to forget the love, the encouragement and the support that I received from my family throughout the process of writing this dissertation. Without your words of wisdom and constructive suggestions, none of this would have been possible.

I dedicate the fruits of my hardwork to The Almighty God and to my family. My mother Margaret Speckman, my father McGlory Speckman, my sisters



Asha and Candice Speckman, my brothers Jerome and Mark Speckman, as well as my sister in-law, Jubilant Speckman. Furthermore, the mother of my daughter Sinomvuzo Marashula, my nephew Amyoli Speckman and my niece Lihle Speckman.

Not forgetting those who were instrumental in my survival of the undergraduate course. I would like to express my sincerest gratitude to Mixo Mushwana, Katamelolo Thabane and Tsholofelo Mashwabi, who were there when I landed on the doorstep of the university as a newbie. This list would be incomplete if I did not include Lindokuhle Gomana, who is one of the critical reasons why I managed to reach the postgraduate level.

Last, but not least, thank you to all the lecturers of the National Diploma in IT and the B.Tech in IT at the Nelson Mandela University. I drew so much inspiration from you all.

# Contents

<b>Declaration</b>	<b>i</b>
<b>Abstract</b>	<b>ii</b>
<b>Acknowledgements</b>	<b>iv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Small, Medium and Micro Enterprises in South Africa . . . . .	2
1.3 Information Security Governance . . . . .	3
1.4 Information Security Requirements . . . . .	5
1.5 Implementing Information Security Best Practices and Standards in SMMEs . . . . .	6
1.6 The Problem Area . . . . .	6
1.6.1 The Problem Statement . . . . .	7
1.6.2 Thesis Statement . . . . .	7
1.7 The Research Objectives . . . . .	8
1.7.1 The Primary Research Objective . . . . .	8
1.7.2 Secondary Research Objectives . . . . .	8
1.8 The Research Design . . . . .	9
1.8.1 The Research Process . . . . .	10
1.9 The Dissertation Layout . . . . .	14
1.10 Delineation . . . . .	16
1.11 Conclusion . . . . .	17

<b>2</b>	<b>Information Security Governance</b>	<b>19</b>
2.1	Introduction . . . . .	19
2.2	Corporate Governance . . . . .	20
2.2.1	The Role of the Stakeholders in Corporate Governance . . . . .	21
2.2.2	The Direct/Control Cycle . . . . .	23
2.3	The Corporate Governance of Information and Communications Technology . . . . .	26
2.3.1	Information and Communications Technology . . . . .	26
2.3.2	The Corporate Governance of ICT Defined . . . . .	26
2.4	Information Security Governance . . . . .	27
2.4.1	Information Security Measures . . . . .	28
2.4.2	Information Security . . . . .	29
2.4.3	Threats to the Characteristics of Information Assets . . . . .	30
2.4.4	How to Direct and Control Information Security . . . . .	34
2.4.5	The Outcomes of Good Information Security Governance . . . . .	37
2.5	Information Security Best Practices and Standards . . . . .	38
2.5.1	Defining Information Security Best Practices and Standards . . . . .	38
2.5.2	Reasons to use Information Security Best Practices and Stan- dards . . . . .	39
2.5.3	Well-known Information Security Best Practices and Stan- dards . . . . .	39
2.6	Information Security Management Systems . . . . .	42
2.6.1	Defining Information Security Management Systems . . . . .	42
2.6.2	The Advantages of Implementing an Information Security Management System . . . . .	43
2.6.3	How an Information Security Management System Works . . . . .	44
2.6.4	An ISO/IEC27001 ISMS . . . . .	44
2.7	Information Security Requirements . . . . .	46
2.8	Conclusion . . . . .	47
<b>3</b>	<b>Information Security Requirements</b>	<b>48</b>
3.1	Introduction . . . . .	48

3.2	Defining Information Security Requirements . . . . .	49
3.2.1	Source 1: The assessment of information security risks to the organisation . . . . .	49
3.2.2	Source 2: Principles, objectives and business requirements . . . . .	50
3.2.3	Source 3: Legal, statutory, regulatory and contractual re- quirements . . . . .	50
3.3	Information Security Best Practices and Standards on Information Security Requirements . . . . .	51
3.3.1	ISO/IEC27003:2010 Information Technology- Security Techniques- Information Security Management System Implementation Guidance . . . . .	52
3.3.2	NISTIR 7621 Small Business Information Security: The Fun- damentals . . . . .	53
3.3.3	NIST SP800-53 Revision 4 (2013) Security and Privacy Con- trols for Federal Information Systems and Organisations . . . . .	53
3.4	Literature on information security requirements . . . . .	55
3.5	Information Security Risk Analysis versus Information Security Re- quirements Analysis . . . . .	56
3.5.1	Information Security Risk Analysis . . . . .	57
3.5.2	Information Security Requirements Analysis . . . . .	59
3.6	Conclusion . . . . .	61
<b>4</b>	<b>Information Security Governance in Small, Medium and Micro Enterprises</b> . . . . .	<b>63</b>
4.1	Introduction . . . . .	63
4.2	Defining Small, Medium and Micro Enterprises . . . . .	64
4.3	SMMEs in South Africa . . . . .	66
4.4	The Importance of SMMEs to the Economy . . . . .	67
4.5	Constraints to the Success of SMMEs . . . . .	69
4.6	The Characteristics of SMMEs . . . . .	70
4.7	The Corporate Governance of SMMEs . . . . .	71
4.8	Information Security Governance in SMMEs . . . . .	75

4.9	Information Security Best Practices and Standards in SMMEs . . . .	77
4.10	The Core Elements of an Artefact for SMMEs . . . . .	79
4.11	Conclusion . . . . .	82
<b>5</b>	<b>The Research Design</b>	<b>84</b>
5.1	Introduction . . . . .	84
5.2	The Research Design . . . . .	85
5.3	Design-oriented IS Research . . . . .	88
5.4	Design-based Research . . . . .	92
5.5	The Integrated Research Design . . . . .	99
5.6	Research Design in Context . . . . .	106
5.6.1	The Analysis Phase . . . . .	107
5.6.2	The Design Phase . . . . .	114
5.6.3	The Evaluation Phase . . . . .	120
5.6.4	The Diffusion Phase . . . . .	125
5.7	The Research Methods . . . . .	128
5.7.1	The Analysis Phase: A Literature Review . . . . .	128
5.7.2	The Design Phase: A Survey, Argumentation, Modelling, Prototyping and Triangulation . . . . .	131
5.7.3	The Evaluation Phase: Expert Interviews . . . . .	133
5.8	Conclusion . . . . .	134
<b>6</b>	<b>A Survey of SA SMMEs</b>	<b>135</b>
6.1	Introduction . . . . .	135
6.2	Step 1: Establish a Theory . . . . .	136
6.3	Step 2: Formulating a Hypothesis . . . . .	137
6.4	Step 3: Selecting the Sample Population . . . . .	138
6.5	Step 4: Collecting the Data . . . . .	140
6.6	Step 5: Analysing the Data . . . . .	144
6.6.1	Filtering the Results . . . . .	145
6.6.2	Scalability . . . . .	148
6.6.3	Simplicity . . . . .	149

6.6.4	Feasibility . . . . .	152
6.6.5	Utility . . . . .	153
6.6.6	Transparency . . . . .	155
6.6.7	Risk Control . . . . .	157
6.6.8	Further Discussions . . . . .	158
6.7	Step 6: Re-evaluating the Hypothesis in Comparison with the Survey Results . . . . .	159
6.8	Step 7: Confirm or Reject the Theory . . . . .	161
6.9	Limitations of the Survey . . . . .	161
6.10	Conclusion . . . . .	162
<b>7</b>	<b>The Alignment of Information Security Requirements</b>	<b>164</b>
7.1	Introduction . . . . .	164
7.2	Deriving the draft principles . . . . .	165
7.3	A framework versus a model . . . . .	168
7.4	PART I: Constructing the MAISRSS . . . . .	171
7.5	The Governance Aspect . . . . .	174
7.6	The Process Aspect . . . . .	178
7.6.1	Enterprise Categorisation . . . . .	180
7.6.2	Objectives Determination . . . . .	181
7.6.3	Asset Identification . . . . .	182
7.6.4	Scope Determination . . . . .	183
7.6.5	Roles and Responsibilities . . . . .	185
7.6.6	Business Impact Analysis . . . . .	186
7.6.7	Gap Analysis . . . . .	188
7.6.8	Information Security Directive . . . . .	191
7.7	Summary . . . . .	193
7.8	PART II: Defining the Automated Tool . . . . .	196
7.9	Automated Enterprise Categorisation . . . . .	196
7.10	Automated Objectives Determination . . . . .	198
7.11	Automated Asset Identification . . . . .	199
7.12	Automated Scope Determination . . . . .	201

7.13	Automated Roles and Responsibilities . . . . .	203
7.14	Automated Business Impact Analysis . . . . .	204
7.15	Automated Gap Analysis . . . . .	206
7.16	Automated Information Security Directive . . . . .	209
7.17	Conclusion . . . . .	213
<b>8</b>	<b>Evaluating the MAISRSS and the Automated Tool</b>	<b>215</b>
8.1	Introduction . . . . .	215
8.2	The Evaluation Approach . . . . .	216
8.3	PART I: Designing the Information Security Expert Interview . . .	219
8.3.1	The Background Information . . . . .	220
8.3.2	The General Principles . . . . .	220
8.3.3	The Draft Principles . . . . .	221
8.4	Analysis and Results of the Information Security Expert Interview .	221
8.4.1	The Background Information . . . . .	222
8.4.2	The General Principles . . . . .	223
8.4.3	The Draft Principles . . . . .	224
8.5	Revisions to the MAISRSS . . . . .	225
8.6	Conclusions Drawn from the Information Security Expert Interview	227
8.7	PART II: Designing the SMME Expert Interview . . . . .	229
8.7.1	The Background Information . . . . .	230
8.7.2	The General Principles . . . . .	230
8.7.3	The Draft Principles . . . . .	231
8.8	Analysis and Results of the SMME Expert Interview . . . . .	231
8.8.1	The Background Information . . . . .	231
8.8.2	The General Principles . . . . .	232
8.8.3	The Draft Principles . . . . .	233
8.9	Revisions to the Automated Tool . . . . .	234
8.10	Conclusions Drawn from the SMME Expert Interview . . . . .	235
8.11	Conclusion . . . . .	236

<b>9 Conclusion</b>	<b>238</b>
9.1 Introduction . . . . .	238
9.2 Summary of Chapters . . . . .	239
9.3 Problems and Challenges . . . . .	242
9.4 Summary of Contributions . . . . .	243
9.5 Suggestions for Future Research . . . . .	249
9.6 Epilogue . . . . .	249
<b>References</b>	<b>250</b>
<b>I Appendices</b>	<b>264</b>
<b>A National Small Business Act of 1996 Schedule</b>	<b>265</b>
<b>B A Survey of SA SMMEs</b>	<b>268</b>
B.1 Request for Participation: The ECITI . . . . .	268
B.2 Request for Participation: Propella . . . . .	273
B.3 The Survey: Questionnaire . . . . .	278
<b>C The Information Security Expert Interview</b>	<b>290</b>
C.1 Information Security Expert Interview: Cover Letter . . . . .	291
C.2 Information Security Expert Interview: Background Information . . . . .	293
C.3 Information Security Expert Interview: Information Security Re- quirements Definition . . . . .	298
C.4 Information Security Expert Interview: Draft Principles . . . . .	304
C.5 Information Security Expert Interview: Questionnaire . . . . .	309
<b>D The SMME Expert Interview</b>	<b>314</b>
D.1 SMME Expert Interview: Cover Letter . . . . .	315
D.2 SMME Expert Interview: Background Information . . . . .	317
D.3 SMME Expert Interview: Questionnaire . . . . .	324
<b>E Academic Publications</b>	<b>330</b>



**F Language Quality Assurance Certificate**

**336**

# List of Tables

4.1	Summary of NSBA Schedule . . . . .	67
4.2	Constraints to the success of SMMEs . . . . .	69
4.3	Characteristics of SMMEs . . . . .	71
4.4	Characteristics of an artefact for SMMEs . . . . .	78
4.5	Characteristics and constraints of SMMEs . . . . .	80
4.6	Mapping The Core Elements and Constraints/Characteristics . . . . .	82
5.1	Research paradigms . . . . .	87
5.2	Design-oriented IS Research . . . . .	90
5.3	Design-based Research . . . . .	97
5.4	Integrated Research Design: Analysis Phase . . . . .	100
5.5	Integrated Research Design: Design Phase . . . . .	101
5.6	Integrated Research Design: Evaluation Phase . . . . .	102
5.7	Integrated Research Design: Diffusion Phase . . . . .	103
5.8	The Integrated Research Design Phases Summary Table . . . . .	105
5.9	Mapping the tasks of the Analysis Phases of the integrated research design in the context of this study . . . . .	114
5.10	Mapping the tasks of Design Phase of the integrated research design in the context of this study . . . . .	119
5.11	Mapping the tasks of the Evaluation Phase of the integrated research design in the context of this study . . . . .	124
5.12	Mapping the tasks of Diffusion Phase of the integrated research design in the context of this study . . . . .	127

6.1	Categories of Questionnaire Respondents . . . . .	149
6.2	Educational Qualifications of Respondents . . . . .	150
7.1	A table of discoveries from the literature review. . . . .	166
9.1	A Summary of the contribution of the chapters of this dissertation .	247

# List of Figures

1.1	Research Process Diagram . . . . .	13
2.1	Diagram of Hierarchical Management Levels . . . . .	22
2.2	The Direct/Control Cycle Diagram . . . . .	25
2.3	Diagram of an ISO/IEC27001 ISMS Development and Implemen- tation Process . . . . .	45
4.1	Flexible and Informal Organisational Structure . . . . .	72
4.2	The SMME Organisational Structure . . . . .	73
4.3	Structured and Hierarchical Organisational Structure . . . . .	74
5.1	Design-oriented IS Research . . . . .	91
5.2	Design-based Research . . . . .	98
5.3	Integrated Research Design Diagram . . . . .	106
5.4	Analysis Phase of integrated research design . . . . .	108
5.5	Three-tiered information security risk management approach. Adapted from NIST SP800-53 R4 (2013, p. 7) . . . . .	110
5.6	The Analysis Phase of integrated research design in the context of this research study . . . . .	113
5.7	Design Phase of integrated research design . . . . .	115
5.8	Design Phase . . . . .	119
5.9	Design Phase of integrated research design . . . . .	121
5.10	Evaluation Phase . . . . .	124
5.11	Design Phase of integrated research design . . . . .	126

5.12	Diffusion Phase . . . . .	127
6.1	Statistician's recommendations . . . . .	142
6.2	Pilot Study Suggestions . . . . .	143
6.3	Information Security Challenges . . . . .	151
6.4	Use of Information Security Best Practices and Standards . . . . .	153
6.5	Ease of Aligning Information Security Requirements . . . . .	156
6.6	Source of Information Security Controls in some SA SMMEs . . . . .	158
7.1	The Theoretical Model . . . . .	172
7.2	The MAISRSS Model . . . . .	174
7.3	The MAISRSS Governance Aspect . . . . .	175
7.4	The Direct/Control Lines of SMMEs . . . . .	177
7.5	MAISRSS Processes Aspect . . . . .	179
7.6	Information Security Gap Analysis . . . . .	189
7.7	The Automated Enterprise Categorisation . . . . .	197
7.8	The Automated Objectives Determination . . . . .	199
7.9	The Automated Asset Identification . . . . .	200
7.10	The Automated Scope Determination . . . . .	203
7.11	The Roles and Responsibilities . . . . .	204
7.12	The Automated Business Impact Analysis . . . . .	205
7.13	The Automated Gap Analysis . . . . .	206
7.14	The Automated Gap Analysis Part 2 . . . . .	208
7.15	The Automated Information Security Directive Process (part 1) . . . . .	210
7.16	The Automated Information Security Directive Process (part 2) . . . . .	211
7.17	The Automated Information Security Directive Process (part 3) . . . . .	212
7.18	The Automated Information Security Directive Process (part 4) . . . . .	213
8.1	The MAISRSS Revised Process Aspect . . . . .	226
8.2	SMME Expert Comments . . . . .	235

# Chapter 1

## Introduction

*“Science starts only with problems”*- Karl Popper

### 1.1 Background

Numerous scholars report that small, medium and micro enterprises (SMMEs) are the backbone of the economy of any nation, and the key to the inclusion of developing countries in the global economy (UNIDO, 2002, p. 3; Koornhof, 2009, p. 17; Ongori & Migiro, 2010; Smit & Watkins, 2012; Valli, Martinus & Johnstone, 2014; Devos, Landeghem & Deschoolmeester, 2011). Like most modern organisations, SMMEs rely consistently on information and communication technology (ICT) in order to store transmit and process information to perform business operations (Posthumus & von Solms, 2004).

The importance of the information to the business operations of the enterprise has made information a valuable asset to an enterprise and to its adversaries. It is not surprising that studies have found that SMMEs have experienced a growing number of attacks on their ICT systems by adversaries who are attempting to access or sabotage the information assets of these enterprises (Feagin, 2015).

Thus, it has become imperative that SMMEs establish the level of security required to adequately protect their information assets against attacks on the

vulnerabilities of the ICT systems used within these enterprises. Moreover, in South Africa (SA), where there were reported to be more than 2 million (2 251 821) SMMEs in the year 2015 (BER, 2016, p. 1).

Thus, this chapter introduces a research study in which a method for SA SMMEs to address the above discussed concern was developed. *Therefore, the purpose of this chapter is to introduce the context of this research study. In doing so, the reader will be introduced to the problem that was investigated in this research study and the process followed to address this problem.*

This chapter begins by introducing the reader to SMMEs in South Africa. Thereafter, the chapter discusses Information Security Governance, while the reader is guided into another discussion about information security requirements. Insight into the use of Information Security Best Practices and Standards in SA SMMEs is given in the fifth section of this chapter. Further sections of this chapter include the Problem Area, the Research Objectives, the Research Design, the Dissertation Layout and the Delineation. Finally, a Conclusion section offers a brief discussion of how the discussions in this chapter have accomplished the purpose of the chapter.

## **1.2 Small, Medium and Micro Enterprises in South Africa**

SMMEs are universally present enterprises, generating employment and contributing to the gross domestic product of economies on a world wide scale (Ayat, Masrom, Sahibuddin, & Sharifi, 2011). However, it is difficult to provide a globally comprehensive definition for what an SMME is. In some instances it is even reported that no such formal definition even exists (Devos et al., 2012). It is further reported that historically this was not a problem; as all organisations were SMMEs. In recent days, a shift from the common family-owned enterprise to larger multi-manager corporations has brought about the need to categorise organisations

(Koornhof, 2009, p. 12). This is even more the case of SMMEs; as these enterprises have unique characteristics, which prevent them from simply being viewed as miniature versions of large organisations (Devos et al., 2012).

As mentioned earlier in this chapter, there were reportedly 2 251 821 SMMEs in SA in the year 2016 (BER, 2016, p. 1). Studies have found that SMMEs in SA contribute over 40 per cent to the GDP of the economy per annum, thereby making them an essential component of the SA economy (Van Niekerk & Labuschagne, 2006). According to the National Small Business Act of South Africa (1996), an SMME is a separate and distinct business enterprise, which includes co-operative enterprises and non-governmental enterprises. Additionally, a number of characteristics of the enterprise are considered to ascertain that the enterprise is indeed an SMME. These characteristics include a maximum of 200 employees and a maximum of 18 million rand in annual revenue (The President's Office, 1996, p. 15).

Thus, some authors believe that SMMEs often have to contend with large organisations, with a fraction of the resources that the large organisations have (Gupta & Hammond, 2005). This is one of the factors that results in the high failure rate of SMMEs especially in SA (Smit et al., 2012). Other factors that affect the survival of SMMEs in developing countries, such as those in SA, are limited financial and human resources, the lack of a skilled labour force (expertise) and the lack of corporate governance skills (Ongori & Migiro, 2010; Dube, Dube, & Mishra, 2011; Abor & Biekpe, 2007).

### **1.3 Information Security Governance**

Von Solms and von Solms (2008, p. 2), define corporate governance as the process of providing an organisation with strategic direction. Furthermore, corporate governance involves verifying that the assets of an organisation are used appropriately and managing the risks to the assets of an organisation. Therefore, risks to the information assets of an organisation, presented by vulnerabilities in the ICT systems, should form part of the corporate governance process also (IoDSA, 2009,



p. 6; OECD, 2015, p. 11; von Solms & von Solms, 2009, p. 1).

Consequently, the management of risks against the information assets of an organisation is the cornerstone of ICT governance. ICT governance is the process of ensuring that the strategic objectives and the information assets of an organisation are not jeopardised by failures or the compromising of the ICT systems of that organisation (von Solms & von Solms, 2008, p. 11). However, it is held that ICT governance is mainly concerned with the protection of the ICT systems used by an organisation, rather than the protection of the information assets housed by these systems. It is claimed that the security of information assets, which can be achieved purely through technical means is limited and should be supported by the management of an organisation by implementing appropriate processes to adequately secure its information assets (ISO/IEC27001, 2013, p. viii).

One such process is information security governance (ISG). ISG is concerned with directing and monitoring the processes and controls that secure the significant characteristics (confidentiality, integrity and availability) of the information assets of enterprises. Thus, ISG goes beyond just technical controls, which protect the ICT systems used by an organisation (ISO27002, 2013, p. 1; von Solms & von Solms, 2009, p. 6). ISG is an on-going process, which must ensure that all information security efforts of the organisation are aligned with the business needs of an organisation and with the relevant laws. More-over, each organisation's complexity is unique and so are the risks of an adversary exploiting the vulnerabilities of its ICT systems (ISO/IEC27003, 2010, pp. 1-3).

Consequently, the establishment and the implementation of efforts to protect the information assets of an organisation are influenced by a number of factors. These factors include the needs and objectives of an organisation, as well as the information security requirements of an organisation (ISO/IEC27001, 2013, p. v).

## 1.4 Information Security Requirements

Information security requirements act as a key factor, influencing the selection of information security controls, to protect the information assets of an organisation (Gao & Zhong, 2015). The selection and implementation of information security controls, for the protection of the information assets of an organisation, are important tasks. Additionally, the selection of information security controls can have major implications on the operations and the information assets of the organisation (NISTSP800-53, 2013). Thus it is important to determine the level of security required to properly protect the information assets of an organisation, without having a negative impact on these operations.

Information security requirements are the result of a combination of the information security concerns and the level of security required for each information asset. Simply stated, the information security requirements for each information asset take into account the level of protection required for each significant characteristic of an information asset (Gerber, von Solms, & Overbeek, 2001). A detailed description of information security requirements will follow in section 3.2 of Chapter 3.

It is reported that information security requirements appear in both technical and non-technical forms. They feature in company policy documents, as well as in information system development requirements; and they have an impact on information security governance in organisations. Therefore, the information security requirements of an organisation should support the business objectives of that organisation; as they are set by the overall corporate governance structure of the organisation (NISTSP800-53, 2013, p. viii). Thus, it is recommended that all organisations establish their unique information security requirements, as proposed by information security best practices and standards (ISO/IEC27002, 2013, p. vi; Gerber & von Solms, 2005; Gerber & von Solms, 2008)

## 1.5 Implementing Information Security Best Practices and Standards in SMMEs

Information security best practices and standards exist, to assist organisations in their information security governance efforts. However, it is reported that the implementation of these best practices and standards can be a costly and overwhelming process (ITGI & OGC, 2008, p. 6). Furthermore, most information security best practices and standards are developed for large organisations, which typically have more resources than SMMEs (Barlette & Fomin, 2008). Even where information security best practices and standards are developed for implementation in SMMEs, they are usually internationally endorsed; and they are not necessarily aligned with local legislative and regulatory requirements (Van Niekerk & Labuschagne, 2006).

This presents a major challenge for organisations, such as SMMEs, which face a number of constraints. These constraints are reportedly due to the unique characteristics of SMMEs. The constraints include a lack of capital finances, and skilled human resources, less frequently seen as constraints of large corporations (Smit et al., 2012).

## 1.6 The Problem Area

*“The precise statement of any problem is the most important step in its solution.” - Edwin Bliss*

This section summarises the above discussions in the context of the research problem identified by this research study. As discussed, information assets reside on ICT systems in most modern organisations. These ICT systems frequently have vulnerabilities, which can be exploited by adversaries of the enterprise, in order to gain access to, or to sabotage the information assets. Information security governance is the process of implementing measures to secure the information assets of the organisation, while ensuring that these measures do not interfere

with the business operations of an enterprise. It is crucial that the information security requirements of an organisation are established. The information security requirements of an organisation are a measure of the level of security required, in order to protect each significant characteristic of its information assets.

Information security best practices and standards offer guidance on establishing the information security requirements of an organisation. However, information security best practices and standards are often too complex and resource intensive to implement in most SMMEs. Even where information security best practices and standards are developed for implementation in SMMEs, they are usually internationally endorsed; and they are not necessarily aligned with local legislative and regulatory requirements. The characteristics of SMMEs in SA are similar to the characteristics of SMMEs found in other parts of the world. Hence, it can be concluded that due to these characteristics, information security best practices and standards are also too complex and resource intensive for SA SMMEs.

### 1.6.1 The Problem Statement

Thus, based on the above summary, the problem statement of this research study can be defined as follows:

*The unique characteristics of SMMEs make the current information security best practices and standards too complex for SA SMMEs to use in establishing the information security requirements aligned to the objectives of the enterprise.*

### 1.6.2 Thesis Statement

Therefore, it is hypothesised that:

*The development of a model based on the unique characteristics of SA SMMEs, would simplify the process of establishing information security requirements aligned to the objectives of these enterprises.*

The research problem, which this research study attempts to address has now been defined. Therefore, the following section will introduce the research objectives which were accomplished to address the research problem.

## 1.7 The Research Objectives

To address the identified research problem of this research study, as defined above, the research objectives were formulated. Research objectives are the goals which must be reached to confirm the thesis statement of a research study. Below are the research objectives of this research study, beginning with the primary research objective.

### 1.7.1 The Primary Research Objective

The primary research objective of this research study is *to develop a model based on the unique characteristics of SMMEs, which would simplify how SA SMMEs establish the information security requirements that are aligned to the objectives of the enterprise.*

To support the primary research objective, four secondary research objectives were formulated. The four secondary research objectives of this research study are listed below.

### 1.7.2 Secondary Research Objectives

To support the primary research objective the following secondary research objectives would need to be accomplished. The four secondary research objectives of this research study are:

- To identify from the literature, what the outcomes of good information security governance are;
- To establish the criteria that define an information security requirement from information security best practices and standards;

- To obtain the perspective of various authors on the use and understanding of information security requirements; and
- To determine the core elements of an information security artefact developed for SMMEs.

To accomplish the research objectives while ensuring that a methodical, structured process is followed, a suitable research design was identified. The following section discusses the research design which was followed throughout this research study.

## 1.8 The Research Design

This research study addresses a real-world practical research problem. Thus, the research study was conducted by following the design-oriented information systems (IS) research approach. Design-oriented IS research aims at the development of artefacts, such as models and methodologies (Österle et al., 2010).

The design-oriented IS research approach has four phases, namely:

1. The Analysis Phase;
2. The Design Phase;
3. The Evaluation Phase; and
4. The Diffusion Phase.

Further guidance in conducting the research study was drawn from integrating design-oriented IS research with design-based research, as defined by Herrington, McKenney, Reeves and Oliver (2007). Design-based research stems from the learning sciences domain; however, it offers similar phases to design-oriented IS research, but with more detailed guidance (Barab & Squire, 2004). The four phases of design-based research, as defined by Herrington, McKenney, Reeves and Oliver (2007), are listed below:

1. Phase 1: The analysis of practical problems by researchers and practitioners in collaboration;
2. Phase 2: The development of solutions informed by existing design principles and technological solutions;
3. Phase 3: The iterative cycles of testing and refinement of solutions in practice; and
4. Phase 4: The reflection to produce design principles and to enhance solution implementation.

The phases of design-oriented IS research and design-based research are discussed in detail in Chapter 5 of this dissertation. Various research methods will be discussed in detail in section 5.7 of Chapter 5; and they form part of the research process, as can be seen in the section below.

### 1.8.1 The Research Process

This section briefly discusses the phases of the integrated research design process followed, in the context of this research study. The four phases are representative of the four phases of design-oriented IS research; while detailed guidance in each phase was taken from design-based research.

1. **Analysis:** A literature review will be used as the primary research method of this research project. The current literature on information security will be consulted to establish the perspective of researchers on information security requirements based on previously conducted research. Information security best practices and standards will provide the necessary criteria to define a valid or adequate information security requirement. The literature on SMMEs and their constraints will assist in identifying the core elements which would make a model suitable for implementation in an SMME environment. Furthermore, the literature will be consulted to establish what the outcomes of good information security governance are.

2. **Design:** The criteria, perspective, outcomes and core elements, obtained from the previous phase, will be used as input for the development of a survey. The survey will be conducted by electronic methods, where an email will be sent to SA SMME owners asking them to participate in the survey. The survey will aim to establish the constraints, which the model must satisfy. Following the analysis of the survey findings, draft principles will be established and used to develop a first draft of the model. The draft principles should not be mistaken for an incomplete or initial version of the principles. Rather, draft refers to the use of the principles to construct (draft) an artefact. A detailed discussion of draft principles features in section 7.2 of Chapter 5. Additionally, an automated tool for SA SMMEs to establish their information security requirements, will be developed as a prototype to demonstrate the practicality of the model.
3. **Evaluation:** An information security expert and an SMME expert will be selected to participate in the expert interviews. The purpose of the expert interviews will be to validate the draft of the model and the automated tool, respectively. After the expert interviews, an analysis and report on the findings will be done. Moreover, recommendations and suggestions of measures to address any issues or shortcomings of the draft of the model will be noted. Similarly, recommendations for refining the automated tool and its implementation will also be addressed.
4. **Diffusion:** The expert interviews will also assist in determining the areas for future research on this topic. Additionally, the write up process of the dissertation will commence in this phase; and the findings will be presented by means of academic publications.

Section 5.5 of Chapter 5, discusses the integrated research design in detail. Furthermore, section 5.6 of Chapter 5 discusses how the integrated research design was followed in the context of this research study. Section 5.7 of Chapter 5, also provides a detailed discussion of the research methods used in the integrated research design. Refer to Figure 1.1 (Research Process Diagram) for a graphical represen-



tation of the research process to be followed throughout this research study, as discussed above. This research process remains iterative; and it shows scientific rigour, with validation and consultation with the concerned parties taking place at various stages of the research process.

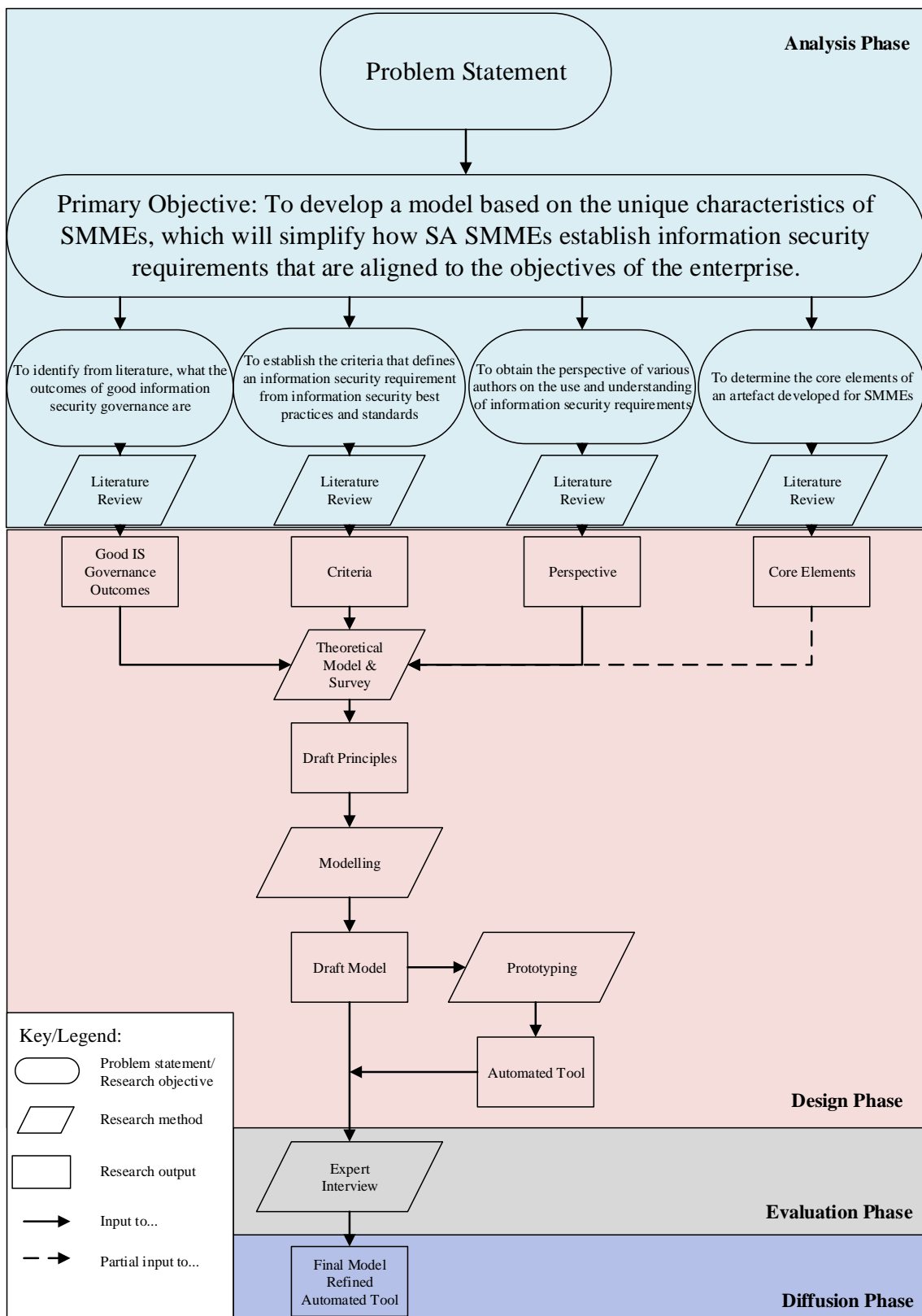


Figure 1.1: Research Process Diagram

Considering the above research process, the structure of this dissertation will be arranged, as can be seen in the following section of this chapter.

## 1.9 The Dissertation Layout

The structure of this research dissertation will follow the order seen below. Each of the chapters of this dissertation will be listed, with a brief discussion on the contents of each chapter. Chapters 2 through 4, attempt to address the secondary research objectives. Chapter 3 addresses two of the secondary research objectives.

### **Chapter 1: The Introduction**

The Introduction provides the reader with the context in which this research study was conducted. The reader is also given a roadmap of the process followed when conducting the research study, and what to expect in this dissertation.

### **Chapter 2: Information Security Governance**

This chapter addresses the first secondary research objective, by reviewing the literature to identify the outcomes of good information security governance. Furthermore, to create the context and understanding, the reader is introduced to corporate governance, as the over-arching governance structure of organisations.

### **Chapter 3: Information Security Requirements**

The chapter continues with the notion of information security governance, advocating for establishment of information security requirements. Thus, the outcome of this chapter is the criterion of an information security requirement, as defined in a number information security best practices and standards. Additionally, this chapter obtains from the literature, what the perspective of various authors is on information security requirements and their use.

**Chapter 4: Small Medium and Micro Enterprises**

This chapter discusses the main subject of this research project, namely SMMEs; and it mentions the characteristics, the constraints and the challenges that SMMEs face. In particular, it mentions the characteristics of SMMEs, which make using information security best practices and standards too complex for these enterprises. The outcome of this chapter produces the core elements of an artefact developed for SMMEs.

**Chapter 5: The Research Design**

This chapter provides the details on how design-oriented IS research and design-based research have formed the integrated research design followed throughout this research study. Furthermore, the researcher defines and discusses how each of the research methods were used to accomplish the research objectives of this research study.

**Chapter 6: A Survey of SA SMMEs**

This is a chapter on the seven step survey conducting process that was followed to design and conduct a survey on a number of SA SMMEs. Moreover, an analysis and discussion of the results of the survey also features in this chapter. Also discussed, is how this survey was also used to verify the applicability of the core elements in the SA SMME environment. The core elements were used as an input to derive the draft principles, which will appear in more detail in Chapter 7.

**Chapter 7: A Model for the Alignment of Information Security Requirements in SA SMMEs**

This chapter guides the reader through the process of deriving the draft principles, which were used to guide the design and development of the model. Additionally, the theoretical model that was initially developed; and its shortcomings in the SMME environment are discussed. The chapter then branches into two parts. In Part I of Chapter 7, the researcher discusses the model that was developed.

Part II of Chapter 7, provides a discussion of the automated tool for SA SMMEs, to determine their information security requirements. The automated tool was developed as a prototype to demonstrate the practicality of the model, as discussed in Part I of Chapter 7.

### **Chapter 8 The Validation of the MAISRSS**

This chapter reports on the analysis and the findings of the results from the expert interviews conducted as part of the validation of the suitability of the model for SA SMMEs. Recommendations and suggestions from an information security expert and an SA SMME expert are discussed, together with some improvements that can be made to the model and the automated tool. This chapter again follows the two part series of discussions, as seen in Chapter 7. The validation of the model is discussed in Part I of Chapter 8; while the validation of the automated tool is discussed in Part II of the same chapter.

### **Chapter 9: Conclusion**

This chapter revisits the research objectives of this research study, and how each of the research objectives was accomplished in the respective chapters. Furthermore, the thesis statement of this research study is reviewed, in order to determine whether the claim of the thesis statement of this research study has been achieved. Future work to be considered on this research field is also discussed in this chapter.

## **1.10 Delineation**

This research project is delineated to SMMEs in South Africa only. The model developed from this research study is focused on simplifying the manner in which SA SMMEs establish information security requirements, which are aligned to the objectives of the enterprise. Information security requirements should not in any way be confused with the requirements of a software application or requirements engineering. SMMEs will be considered as a whole; and no specific category of SMME (small, medium or micro) will be focused on.

Due to the limited number of survey responses received, no statistical inferences were drawn from the results of this study. This is in no way a statistical or quantitative study; and any references to statistical terms should not be considered as such. Additionally, enterprises in this context are used to refer to SMMEs, unless otherwise stated. Where any instances of the term *organisation* appears, the researcher refers to large corporations and to SMMEs collectively. This research study does not adhere to the positivist research paradigm.

Although it is noted as a concern in this dissertation, this research study does not address, design, or develop any information security awareness campaign. In reviewing the literature, the researcher did review the Soft Systems Methodology by Checkland and Poulter (2010). However, the Soft Systems Methodology does not relate to the same objectives as does the model developed in this research study. Soft Systems Methodology refers to a process which can be used for determining the information security requirements of a system to be developed, by a process similar to requirements engineering.

## 1.11 Conclusion

The purpose of this chapter was to introduce the reader to the context of this research study. In doing so, the researcher intended to introduce the research problem, which has been addressed in this research study.

Therefore, in this chapter, it was discussed that SMMEs play an important role in the economy of any nation, including SA. Similar to most other organisations, SMMEs make use of information that is critical to the business operations of the enterprise. The criticality of the information to the business operations of the enterprise, make it an asset. Frequently information assets are stored, created and transmitted by using ICT systems. However, these ICT systems have vulnerabilities that can be exploited by adversaries to gain access to the information assets or to sabotage them.

Therefore, the management of the enterprise should implement information

security governance measures as part of the corporate governance of the enterprise. For this reason, the unique information security requirements of the enterprise should be established. It was found that due to their complex nature, information security best practices and standards are often not easily implemented in SMMEs. Thus, the problem statement of this research study was defined, as may be seen in section 1.6.1 of this chapter.

Notwithstanding the above, it can therefore be concluded that this chapter accomplished its intended purpose, as defined in section 1.1 of this chapter. The following chapter (Chapter 2), offers an in-depth discussion of information security governance.

# Chapter 2

## Information Security Governance

*“A man who reviews the old so as to find out the new is qualified to teach others.”- Confucius*

### 2.1 Introduction

As defined in section 1.3 of Chapter 1, information security governance is an ongoing process. Moreover, this process entails ensuring that the information security efforts of an organisation are aligned with its business needs and the relevant laws of the land. Consequently, the objective of this chapter is ***to identify the outcomes of good information security governance.***

This chapter begins by defining corporate governance and its stakeholders in an organisation. The chapter goes on further to discuss the direct/control cycle of corporate governance. A later section attempts to define the corporate governance of information and communications technology (ICT). This is followed by a definition of information security governance, which entails discussing information security controls, information security and information security threats. Further sections discuss the outcomes of good information security governance, information security best practices and standards, as well as information security management systems. Finally, a brief introduction to information security requirements is given, before the concluding section of the chapter.



## 2.2 Corporate Governance

Corporate governance can be defined as the process exercised by the stakeholders of an organisation, to set the organisational strategy. The organisational strategy should be established by the strategic-level managerial team of an organisation; and it must define the path required to achieve the objectives of that organisation, while ensuring that the assets of the organisation are used in an efficient and effective manner (OECD, 2015, p. 9; von Solms & von Solms, 2009, p. 2). The Organisation for Economic Co-operation and Development is abbreviated to OECD throughout this dissertation. A few instances of the unabbreviated name may appear in later chapters, for the convenience of the reader.

The use of an organisations assets to achieve the objectives of the organisation, is the responsibility of all the stakeholders of that organisation. Therefore, the corporate governance of an organisation involves all of that organisations stakeholders, namely (von Solms & von Solms, 2008, p. 2):

- The Board of directors (the Board): The roles and responsibilities of the board include steering the organisation and setting its strategic direction, through which, management will develop the strategy;
- The Managers: Once the strategy has been approved by the board, management formulates the policy and the operational plans, which must be approved by the Board, before they are implemented;
- The Workers: The strategy is then implemented and executed by the employees, in accordance with policy and plans; and
- The Shareholders or owners: They are those who have invested resources in the organisation with the hope of receiving a return on their investment in various forms.

The well-being of an organisation and the use of its assets is the responsibility of all of its stakeholders. Each of these stakeholders has a specific role in the

organisation. The roles of stakeholders can be characterised into three main levels, as discussed in the section that follows.

### 2.2.1 The Role of the Stakeholders in Corporate Governance

As mentioned in the previous section, the implementation of the corporate governance strategy is generally overseen by the stakeholders. The stakeholders occupy positions, which can be grouped into three management levels, as seen below (von Solms & von Solms, 2009, p. 3; Whitman & Mattord, 2012, p. 43):

- The Strategic-Level Management lays out the long-term direction to be taken by the organisation. Planning at this level guides organisational efforts and focuses the resources towards specific goals. Guidance is conveyed through the strategic-level directives. At this level, the Board of directors and the executive management of the organisation are to be found, including the CEO of the organisation;
- Tactical-Level Management planning has a more short-term focus than strategic planning, usually one to three years. Tactical-level management translates each applicable strategic plan into a series of incremental objectives. These objectives are reflected in policies and company procedures at the tactical level. Management at this level includes senior- and middle-management; and
- Operational-Level Management, lower-management, supervisors and administration use operational plans to organise the on-going, day-to-day performance of tasks. The operational plan includes the identified co-ordination activities that span departments, communication requirements, weekly meetings, summaries, progress reports and associated tasks. Operational plans must reflect the organisational structure, with each department or project team conducting its own operational planning and reporting components.

The three management levels discussed above can be graphically represented by means of a diagram (see Figure 2.2.1).

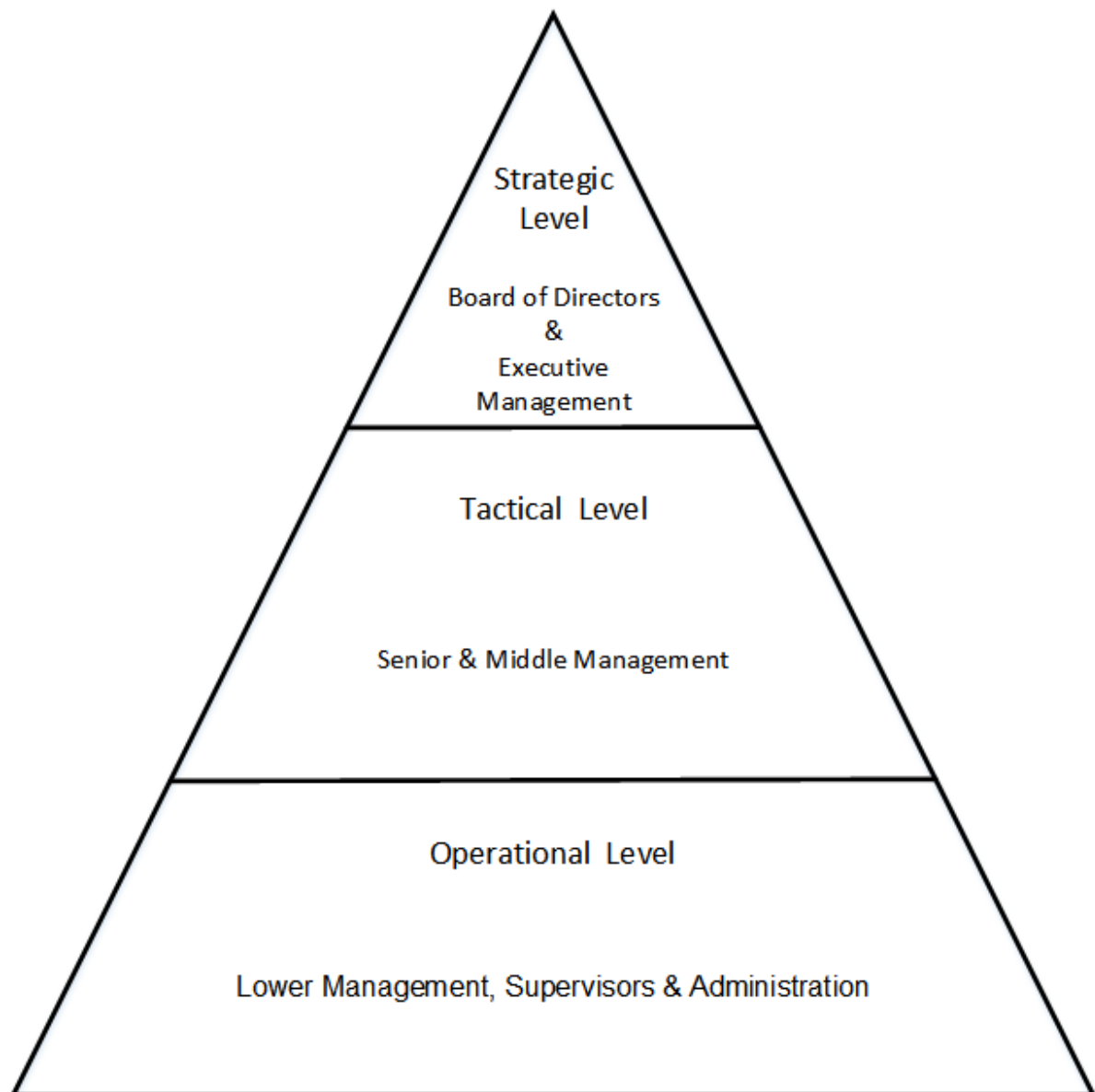


Figure 2.1: The Corporate Governance Hierarchical Management Levels. Adapted from Coertze & von Solms (2013)

The stakeholders of an organisation perform the corporate-governance process by issuing instructions aligned to its objectives and evaluating the compliance with

these instructions. This forms a cyclical process (Eds. Tipton & Krause, 2006, p. 183; von Solms & von Solms, 2009, p. 3), as discussed in section 2.2.2.

### **2.2.2 The Direct/Control Cycle**

In the corporate governance process, an organisation will continuously evaluate its performance, in accordance with its objectives; and it will implement measures to accomplish those objectives, where necessary (Eds. Tipton & Krause, 2006, p. 183; von Solms & von Solms, 2009, p. 3). Organisational objectives are specified through corporate directives and compliance with these organisational objectives is measured in the control of the organisation. Therefore, the corporate governance process is commonly referred as being performed through the direct/control Cycle (von Solms & von Solms, 2009, p. 3). This section will briefly discuss the three phases of the corporate governance direct/control cycle.

#### **Direct**

In this phase, the strategic-level management, going downwards gives guidance to the organisation in the form of documents, such as directives, policies, company standards and procedures. These documents drive and prescribe the execution of business at the lower levels of management (von Solms & von Solms, 2009, p. 3).

#### **Execute**

The execute phase of corporate governance is done by operational-level managers and employees (workers), implementing operational plans, which are derived from the tactical-level management plans, and guide the performing of day-to-day activities of the organisation (Whitman & Mattord, 2012, p. 45).

#### **Control**

Control of the organisation is done by the strategic-level management ensuring that the organisational plans that were set out by the strategic-level management,

are being complied with. This is done by reports of organisational performance being propagated from operational-level management, to tactical-level management and further reports to strategic level management. In this way, the strategic-level management ensures that the organisational directives are actually being complied with. This can also be interpreted as strategic-level management's way of monitoring that outcomes are in accordance with the strategic plans and the mission/business goals and objectives that the organisation has set out to achieve (von Solms & von Solms, 2009, p. 4).

Frequent communication and feedback from the project teams and departments is given to project managers and team leaders. This feedback is then propagated up to the various management levels within the organisation (Whitman & Mattord, 2012, p. 45). The Board ensures that there is accountability for organisational performance, through reporting and disclosure from the strategic-level managers (King Committee, 2016, p. 21).

Figure 2.2.2 graphically depicts the phases of the direct/control cycle, as discussed above.

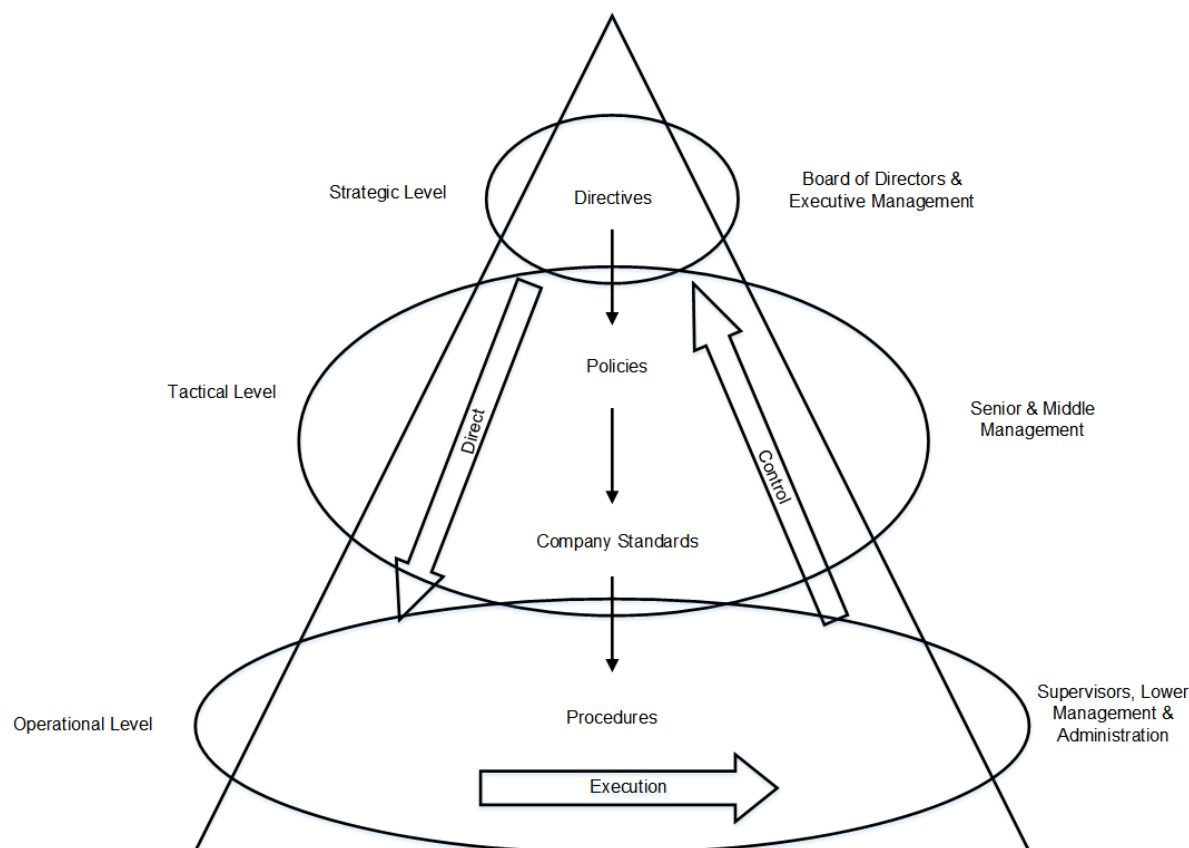


Figure 2.2: The Direct/Control Cycle. Adapted from von Solms & von Solms (2008, p. 3)

Based on the above discussion, it can be concluded that corporate governance is the ongoing process of ensuring that an organisation implements the strategy to achieve its objectives. Furthermore, the corporate-governance process ensures that the assets of an organisation are used efficiently and effectively.

Delpont, von Solms and Gerber (2015), report that many modern day organisations make use of information and communication technology (ICT) systems to support and achieve the objectives of the organisation. Hence, the ICT systems of most organisations are considered as an asset; and they should therefore be governed similarly to the other assets of an organisation.

## **2.3 The Corporate Governance of Information and Communications Technology**

The previous section of this chapter was a discussion on corporate governance and what it entails. The section concluded by stating that ICT should be governed like any other organisational assets. Therefore, this section will define ICT, followed by a discussion on the corporate governance of ICT.

### **2.3.1 Information and Communications Technology**

Zuppo (2012), claims that the diverse applications of ICT make it difficult to provide a universal definition of the concept. An attempt at such would be that in its simplest form, ICT, refers to data networks, databases, computers, servers and other information and communications technology infrastructure (von Solms & von Solms, 2009, p. 6). From a business or management perspective, ICT is simply a set of mechanisms to process, transport and store information. This definition disregards whether the processing, transporting and storage is done by automated machinery or by human processes; as it does not have a major impact on the value or usefulness of the resultant activities (Brotby, 2009, p. 2). ICT systems are used by organisations to support and achieve their objectives. The use of ICT has benefits, such as providing an organisation with a competitive advantage and being an enabler for the organisation to survive. This is true; since ICT has a huge impact on the delivery of services; and it should, therefore, be governed as an organisational asset (Delpont et al., 2015; Wu, Straub, & Liang, 2015).

### **2.3.2 The Corporate Governance of ICT Defined**

ISO/IEC38500 (2015), defines the corporate governance of ICT as the system by which the current and future use of ICT is directed and controlled. Furthermore, the corporate governance of ICT involves providing guidance in the form of strategies and policies for using ICT within an organisation, to support the organisation

in achieving its business objectives and goals (ISO/IEC38500, 2015, p. 3). At its core, the corporate governance of ICT is concerned with two main tasks (Tipton & Krause, 2006, p. 184):

- To ensure that ICT is delivering value to the business; and
- Mitigating the ICT risks that an organisation faces.

As mentioned above, ICT governance pertains to the mitigation of ICT risks, which is to a large extent quite technical (ISO/IEC27001, 2013, p. viii). Similarly, it has been reported that ICT is by definition technology-centric (Gerber, 2001). However, the security that can be achieved purely through technical means is limited (ISO/IEC27002 & ISO/IEC27001, 2013, p. viii). Consequently, it is claimed that the mitigation of ICT risks (and therefore ICT governance) does not address the broader issue of information security governance (Brotby, 2009, p. 2; Gerber & Von Solms, 2001).

## 2.4 Information Security Governance

As mentioned in Chapter 1, information security governance goes beyond the mitigation of risks to the ICT systems of an organisation (Brotby, 2009, p. 2; Gerber & Von Solms, 2001). Information security governance is about setting strategic objectives for the information security of an organisation. These strategic objectives should be in compliance with law, business objectives and industrial regulations relevant to the organisation. Furthermore, information security governance includes evaluating the performance of information security measures (also called information security controls), which go beyond the mitigation of risks to the ICT systems of an organisation and allocating resources for such measures to be applied, where required (von Solms & von Solms, 2008, p. v).

The governance of information security, similarly to corporate governance, is the responsibility of an organisation's strategic-level management (King Committee, 2016, p. 62). Furthermore, information security governance is about the setting of strategic objectives and allocating resources; so that information security



measures are implemented to protect the informational assets of the organisation, in accordance with the laws, business objectives and industrial regulations; and evaluating the performance of the implemented information security measures to ensure that they are operating, as intended (von Solms & von Solms, 2008, p. v).

### 2.4.1 Information Security Measures

Information security measures or controls include the hardware, software, policies, procedures, law and other efforts to counter vulnerabilities, which could potentially result in the compromise of an organisation's information assets (Calder, 2009, p. 3). Information or information assets can be defined as all the data of useful meaning to an organisation. These can be in the form of paper records, electronic media or the personal knowledge of employees (DTI, 2006, p. 3, Brotby, 2009, p. 7).

Examples of information include proprietary information, such as research, customer lists, bids and proposals. Additionally, an organisation may also hold personal, medical and financial information, among others. The nature of information, as seen above, makes it the asset of an organisation; and it is therefore critical for the organisation to survive and thrive (Eds Tipton & Krause, 2006, p. 5; Brotby, 2009, p. 7). The value of information goes beyond the written words, numbers and images that it may contain (ISO/IEC27002 & ISO/IEC27001, 2013, p. viii). The true value of information assets depends on the state of their significant characteristics (Gerber, 2001). When a characteristic of an information asset changes, the value of that information asset either increases, or more commonly, it decreases (Whitman & Mattord, 2012, p. 11). Therefore, the protection of the state of the significant characteristics of information assets is important. This is accomplished through a component process of information security governance, known as information security (von Solms & von Solms, 2008, p. vii).

### 2.4.2 Information Security

As defined in an earlier section, information security governance involves evaluating the performance of information security measures and allocating resources for the implementation of such measures, where required. Also discussed previously, is that information security measures include all efforts implemented to counter vulnerabilities that could result in the compromising of an organisation's information assets.

Security is defined by Whitman and Mattord (2012, p. 8), as the state of being free from danger. Danger in this context refers to the consequences of adversaries who can exploit the vulnerabilities of an organisation to harm it either intentionally, or unintentionally. The consequences referred to in this context include a compromising of the significant characteristics of information assets, decreasing their value, and ultimately thereby affecting the organisation.

Having established the above, it can be concluded that information security is defined as the implementation of measures for the protection of the significant characteristics of the informational assets of an organisation. Therefore, information security should include the protection of systems and hardware that use, store, and transmit those informational assets (Whitman & Mattord, 2012, p. 8).

Various authors have defined those significant characteristics, which make information assets valuable to an organisation. However, most authors define the following as the most significant characteristics of an information asset that should be protected (Whitman & Mattord, 2012, p. 12; Andress, 2014, p. 6):

- Confidentiality is the ability to protect information from disclosure or exposure to unauthorised individuals or systems. In other words, only those with the rights and privileges to access the information are able to do so. Although closely related to privacy, they are not the same;
- Privacy/Possession refers to the quality or state of ownership or control of information. In simpler terms, the information owners can be sure that their

information will only be used for the purpose that they agreed on, when they provided the information;

- Integrity refers to the ability to prevent information from being changed in an unauthorised or undesirable manner. The integrity of information could be compromised by an unauthorised change or the deletion of information or portions thereof; or it could even occur through authorised, but unwanted changes being made to the information. Thus, to maintain the integrity of information, one should be able to both, prevent unauthorised changes to information and undo authorised, but unwanted changes to the information;
- Availability is the characteristic of information that enables an authorised user to have access to information in a usable format, without interference or obstruction, when it is needed. The availability of electronic information assets can be compromised by a number of incidents, such as power loss, operating systems or application problems and network attacks, just to name a few;
- Authenticity of information refers to the quality or state of being genuine, or original, rather than a reproduction or fabrication. This means that information is authentic, when it is in the same state as that in which it was created, placed, stored or transferred; and
- Utility refers to the quality or state of the information having value for some purpose or end. If information is available, but not in a format that is meaningful to the end-user, then it is not useful.

### **2.4.3 Threats to the Characteristics of Information Assets**

The previous section of this chapter defined information security as protecting information assets from threats to the characteristics of the information. This section will discuss a few common threats to the characteristics of information assets. Additionally, this section includes a discussion on information security

attacks, the impact of information-security attacks, the vulnerabilities of information assets, the risks to information assets, as well as information-security control strategies.

### **Attacks**

An organisation might face attacks from intruders, or even insiders trying to gain access to sensitive information. Attacks on the information assets of an organisation can generally be categorised into one of four categories, as described below; and these can affect one or more of the characteristics of information assets. The four categories of attacks are (Andress, 2014, p. 9):

- **Interception:** if this type of attack is successful, unauthorised users gain access to information, or information systems. This attack primarily targets the confidentiality of an informational asset;
- **Interruption attacks** target the usability, or the availability of the information assets on a temporary or permanent basis. Interruption attacks usually affect the availability; but they can be an attack on integrity too;
- **Modification attacks** involve tampering with information assets. This could primarily be viewed as an integrity attack; but it might include an attack on the availability of information assets; while
- **Fabrication attacks** involve generating information, processes, communications, or other similar activities with a system. Therefore, this attack primarily targets the integrity of an informational asset; but it could likewise be viewed as an attack on the availability of the informational assets.

### **Threats**

It is good to know that information security attacks occur and the categories of the attacks that occur. The probability that an attack may occur is known as a threat. A threat is an undesirable event that, if successful, could impact the

organisation's mission or business objectives. Three main categories of threats to informational assets exist (Peltier, 2005, p. 18):

- Natural threats, such as floods, earthquakes, tornado, landslides, avalanches and other such events;
- Human threats: these refer to events that are either enabled or caused by human beings. These could be unintentional acts (e.g. errors and omissions), or deliberate acts (e.g. fraud, malicious software and unauthorised access); and
- Environmental threats; and examples of these include long-term power outages, pollution, chemical spills, liquid leakage and others. Threats to the information assets of an organisation attack can affect one or more of the vulnerabilities of the system, which houses the informational assets.

### **Vulnerabilities**

The threat of an attack occurring is a known possibility to the organisation. Once the attack occurs, the likelihood of the attack actually being successful depends on the vulnerability of the information assets. Vulnerabilities can be defined as the holes that can be exploited by threats, or attacks, in order to cause harm to the information assets. Information assets may be hosted by a system with vulnerabilities; however, this does not guarantee that an attack will be successful. A vulnerable system does, however, increase the risk of an attack being successful (Andress, 2014, p. 11).

### **Risks**

An attack or threat thereof might occur, but until the attack has been successful in harming the information assets, it is only known as a risk. Risk is the likelihood that something bad will happen. A risk is not present until both a threat and the vulnerability co-exist for the threat to exploit the asset. For example, setting a wood structure on fire would present a risk of the structure burning down. Both the

threat (the fire) and the potential vulnerability (the wood structure) exist in the same environment. Risks of threats successfully exploiting the vulnerabilities of an organisation's information systems are quantified, by estimating the potential impact that a successful threat might have on the organisation (Andress, 2014, p. 11).

### **Impact**

A very real risk of a threat exploiting a vulnerability and materialising might exist; but an organisation may choose to ignore this risk, if the impact of the threat is not significant. Accordingly, an organisation might not consider a threat a risk, if the impact of the threat is not of disruption or major loss to the organisation. Impact is sometimes viewed from the perspective of the value of the threatened informational asset, or the level of potential disruption it would have on the business or the mission objectives of an organisation. As an example, the compromising of sensitive information that could result in an organisation going out of business, paying a huge fine, or losing a large number of clients might be considered a risk of significant impact on that organisation (Andress, 2014, p. 12).

In order to properly secure their informational assets, an organisation's strategic-level management must integrate information security practices into the business processes of the organisation. This means that the corporate governance policies and controls should encompass the objectives of the information security process. For this reason, information security is only effective and sustainable when addressed at the highest levels of an organisation's management (Whitman & Mattord, 2010, p. 49; Calder, 2009, p. 27; Von Solms & Von Solms, 2009, p. 17). The section that follows will discuss how strategic management conducts information security governance in a direct/control cycle similar to that of corporate governance.

#### 2.4.4 How to Direct and Control Information Security

The responsibility for ensuring that prudent and reasonable measures have been taken, with regard to information security governance, ultimately resides with the strategic-level management of an organisation (IoDSA, 2009a, p. 18; IoDSA, 2009b, p. 41; Von Solms & Von Solms, 2009, p. vii). Therefore, this section will briefly discuss the structure through which strategic management ensures that these steps have indeed been taken. As previously stated, comprehensive information security governance practices should include strategic direction for information security and activities to ensure compliance with the strategic directives. This requires the participation of all three management levels (strategic, tactical and operational) in the information security governance process (Von Solms, Thomson, & Maninjwa, 2011). The responsibility for directing and controlling information security includes each of the three corporate governance management levels:

##### **Strategic-Level Management**

Strategic-level management sets the organisations information security objectives and gives guidance on what needs to be done, in order to achieve these objectives. The directives are usually based on a number of factors, including the strategic vision of the organisation, the legal and regulatory prescriptions, the role of ICT and its alignment with the organisations strategy and competitiveness. These directives are usually expanded into a corporate information security policy (CISP), or simply an information-security policy. The purpose of an information security policy at this level is to set the information security objectives of the organisation. These are normally the highest level of information-security policies. The CISP, along with the management directives, resides at the strategic-management level. In measuring compliance, the strategic management relies on reports that are propagated from the two lower levels of management (tactical and operational) (Von Solms et al., 2011).

### **Tactical-Level Management**

Tactical management usually expands the strategic-level policies into a series of more detailed information-security policies that are aligned with the information security objectives of the organisation. These policies often include or are referred to as issue-specific policies. Issue-specific policies provide detailed instructions on the use of the organisation's processes, technologies or systems. Policies at the tactical level are usually supported by associated procedures or even organisational standards. Tactical-level managers propagate the specific reports of compliance, received from the operational level (Von Solms et al., 2011).

### **Operational-Level Management**

Operational management implements the issue-specific policies, received from tactical management. The operational management level often has its own procedures that accompany the operational-level policies; detailing how employees should conduct themselves daily, to comply with the issue-specific policies. At this level, policies can target different audiences, such as end-users and technical personnel active at the operational-level. They are mostly differently planned or structured than higher level policies. The control aspect of information security governance is usually a technical analysis of metrics, such as logs from information systems implemented in the organisation (Von Solms et al., 2011).

Directing and controlling information security governance as discussed above, is known as the top-down approach, in which the call for information security comes from the strategic-level management of the organisation (Whitman & Mattord, 2012, p. 20). The next section will briefly discuss the top-down approach, as well as another information security implementation approach.

### **Information Security Implementation Approaches**

The previous section of this chapter discussed the implementation of information security, as initiated by the strategic-level management of an organisation. The section concluded that this approach is one of two main approaches. These two



approaches will briefly be discussed in this section.

### **The Top-down Approach**

In the top-down approach, the project is initiated by upper-level managers, who issue policy, procedures and processes, dictate the goals and the expected outcomes and determine the accountability for each section of the project. Advantages of the top-down approach often include (Whitman & Mattord, 2012, p. 20):

- Strong upper-management support;
- A dedicated champion;
- Dedicated funding;
- Clear planning;
- Implementation process; and
- Means of influencing organisational culture.

### **The Bottom-up Approach**

Contrary to the top-down approach, the bottom-up approach exists, in which information security can begin as a grass-roots effort. In the bottom-up approach, system administrators attempt to improve the information security of their systems, without a call from top management to implement information security. An advantage of the bottom-up approach is that administrators work with their systems on a daily basis; and they therefore possess the technical expertise and in-depth knowledge about threats to their systems and the mechanisms needed to protect them successfully. However, this approach seldom works; as it lacks a number of critical features, such as participant support and organisational staying power from the employees of an organisation (Whitman & Mattord, 2012, p. 20).

Information security governance is often reported to be a tedious process (Vermeulen & von Solms, 2002; Whitman & Mattord, 2012, p. 32). However, it

is reported that there are a number of beneficial outcomes of good information security governance, as will be seen in the next section.

### 2.4.5 The Outcomes of Good Information Security Governance

The outcomes that an organisation should observe when implementing an effective information security governance plan include (Brotby, 2009, p. 6; Whitman & Mattord, 2012, p. 49):

- Strategic alignment of information security with business strategy, to support the organisational objectives;
- Risk management by executing appropriate measures to manage and mitigate risks and reduce their potential impact on information resources to an acceptable level;
- Resource management by utilising information security knowledge and infrastructure efficiently and effectively;
- Performance measurement by measuring, monitoring and reporting information security governance metrics, to ensure that organisational information security objectives are being achieved;
- Value delivery by optimising information security investments in support of organisational objectives; and
- Although it is not mentioned by Whitman and Mattord (2012, p. 49), Brotby (2009, p. 6) claims that business process assurance/convergence is an outcome of good information security governance, achieved by integrating all relevant assurance processes to maximise the effectiveness and efficiency of security activities.

The governance of information security has been reported frequently to be a complex process (Vermeulen & Von Solms, 2002). For this reason a number of recognised and approved sources and information security techniques have been

developed to provide sound technical information security advice. Information security best practices, standards and other tried and trusted methods can minimise the level of guess work involved in securing an organisations information assets (Whitman & Mattord, 2012, p. 32).

## **2.5 Information Security Best Practices and Standards**

Section 2.4.5, concluded by mentioning that information-security best practices, standards and guidelines attempt to provide guidance on the governance of information security, in order to eliminate guess work. This section of the chapter will briefly define information security best practices and standards; it will give a few reasons to use them, as well as discussing a few of the well-known best practices, standards and guidelines, related to information security governance.

### **2.5.1 Defining Information Security Best Practices and Standards**

Information security best practices and standards play a major role in assisting organisations to develop and maintain organisational information security. By adopting an authoritative guideline, organisations can demonstrate their commitment to secure business practices (Siponen & Willison, 2009). They document the knowledge and experience of a group of people (usually organisations), in a particular field, in this case information security governance. Best practices and standards, attempt to answer the question often asked when designing any system: How do I know that I am doing it right?. They also aim to circumvent ‘re-inventing the wheel’, by providing guidelines to design and implement systems based on the knowledge and past experiences of those with reason to be considered experts in the field (von Solms & von Solms, 2008, p. 40).

### **2.5.2 Reasons to use Information Security Best Practices and Standards**

Legally, certain organisations may be compelled to adopt a stipulated minimum level of information security. Organisations that adopt a minimum level of information security, to protect themselves from future legal liability, may need to verify that they have adopted a good-enough level of information security, as would any other organisation in similar circumstances. This is known as due care. Implementing and maintaining a minimum level of information security is known as due diligence. Standards of due care stipulate the minimum strategy that an organisation must implement and maintain, to avoid legal liability (Whitman & Mattord, 2012, p. 249).

Information security best practices and standards can be seen as the information security wheel, invented, tried and tested by other people. It, therefore, provides a reference framework to ensure that all information security bases are covered; as also are any attempts to prevent the reinvention of the information security wheel (von Solms & von Solms, 2008, p. 20). The next section will briefly discuss five of the well-known information-security best practices and standards.

### **2.5.3 Well-known Information Security Best Practices and Standards**

As mentioned at the end of the previous section, this section will discuss five well-known information security best practices and standards. This list is not exhaustive of the most common information security best practices and standards that are available. However, it presents brief discussions on five of the most commonly used ones. Each brief discussion mentions the author (referring to an organisation, not an individual) of the information-security best practice or standard and what its objective is.

### **The CCTA Risk Analysis Management Method**

The CCTA Risk Analysis and Management Method (CRAMM) was created by the Central Computer and Telecommunications Agency (CCTA), now the Office of Government Commerce. The first releases of CRAMM, were based on the best practices of British government organisations. Therefore, CRAMM is reportedly most appropriate for large organisations, like government bodies and industry. Thus, the use of CRAMM is difficult without the related supporting CRAMM tool (ENISA, 2016).

### **Control Objectives for Information and Related Technology**

Control Objectives for Information and Related Technology (COBIT) is a comprehensive framework, published by Information-Technology Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA), for developing, implementing, monitoring and improving ICT governance and management practices (Laksono & Supriyadi, 2015). Simply stated, COBIT, helps enterprises create optimal value from ICT by maintaining a balance between realising benefits and optimising risk levels and resource use. Furthermore, it enables ICT to be governed and managed in a holistic manner for the entire organisation. COBIT 5, the latest version of the framework, is reportedly generic and useful for organisations of all sizes, whether commercial, not-for-profit or in the public sector (Isaca, 2012, p. 13).

### **National Institute of Standards and Technology Special Publication 800-53**

The National Institute of Standards and Technology (NIST), develops and issues standards, guidelines and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002. The NIST Special Publication (SP) 800-53, provides a catalogue of security and privacy controls for federal-information systems and organisations. This standard also provides a process for selecting controls to protect the informational assets of an

organisation (NISTSP800-53, 2013, p. iii).

### **ISO/IEC27000 Series of Standards- Information Security Management Systems**

The ISO/IEC 27000 series is a series of standards, developed by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC) Joint Technical Committee. This series of standards provides a model for organisations to follow in setting up and operating an information security management system (ISMS). Therefore, it is also known as the Information Security Management System family of standards. Through the use of this series of standards, organisations can develop and implement a framework for managing the information security of their informational assets. The standards can also be used to prepare for an independent assessment of their ISMS. The ISO/IEC 27000 series of standards is intended to assist organisations of all types and sizes in implementing and operating an ISMS (ISO27000, 2012).

### **Operationally Critical Threat, Asset and Vulnerability Evaluation**

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) is a risk-based strategic assessment and planning technique for security. The technique leverages peoples knowledge of their organisation's security related practices and processes to capture the current state of security practice within the organisation. Risks to the most critical assets are used to prioritize areas of improvement and to set the security strategy for the organisation. OCTAVE was developed for large organisations with 300 or more employees, and a hierarchical management structure. However, the OCTAVE-S method was developed for small organisations, with a minimum of 20 to 80 employees (Alberts, Dorofee, Stevens, & Woody, 2005).

The implementation of information security best practices, standards and guidelines does not guarantee that information-security incidents will no longer occur (von Solms & von Solms, 2008, p. 40). Rather, information security best practices and standards recommend that organisations develop an information security man-

agement system (ISMS). As such, a system will provide a structured architecture of measurable information security goals and adequate information security controls to meet these goals (IoDSA, 2009, p. 41; ISO/IEC 27002, 2013, p. viii). The next section of this chapter will further discuss information security management systems.

## 2.6 Information Security Management Systems

As mentioned in the previous section, information security best practices, standards and guidelines do not entirely eliminate the chance of information security incidents occurring. However, implementing a structured approach to information security is more effective; as the efforts are measurable and the process is repeatable. This section endeavours to define what an information security management system is, how it can benefit organisations; and it also discusses an ISMS based on the ISO 27000 series of standards.

### 2.6.1 Defining Information Security Management Systems

An information security management system (ISMS) is the overall framework of guidelines, policies, procedures, processes and associated resources of an organisation, aimed at ensuring that the organisation meets its information security objectives. An ISMS is based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security within an organisation (ISO27000, 2012, p. 5). Furthermore, an ISMS also includes organisational structure, planning activities, responsibilities, people and ICT systems, in a coherent, structured management approach to information security (Calder, 2009, p. 3; ISO/IEC 27000, 2012, p. 5).

### 2.6.2 The Advantages of Implementing an Information Security Management System

An ISMS takes a holistic, co-ordinated approach and view of an organisations information security risks, with the aim of understanding the organisation, to implement a comprehensive suite of information security controls under the organisations overall management system (ISO/IEC27001, 2013, p. viii). An organisation should develop an ISMS to ensure the effective interaction between the three key attributes of information security, these being (Calder, 2009, p. 3):

- Processes;
- Technology; and
- Behaviour (the human aspect).

Calder (2009, p. 4) further states that there are four reasons for an organisation to develop and implement an ISMS:

- Strategic: Due to a government or parent-company requirement, or a strategic board decision to better manage the organisations information security, in the context of its overall business risks;
- Customer confidence: This refers to the need to demonstrate to one or more customers that the organisation complies with information-security best practices, in an attempt to gain a competitive advantage over its competitors, with regard to customer and supplier relationships;
- Regulatory: The desire to meet various statutory and regulatory requirements particularly around the misuse of ICT, information protection and personal privacy; as well as
- Internal effectiveness: The desire to manage information more efficiently within the organisation.



The implementation of an ISMS will not automatically confer the organisation immunity from legal obligations. Organisations must also ensure that they understand the range of legislation and regulation with which they must comply. These organisations must likewise ensure that the requirements are reflected in the ISMS; as it is developed and implemented. And then they must ensure that the ISMS works as it was designed to work (Calder, 2009, p. 4).

### **2.6.3 How an Information Security Management System Works**

An ISMS provides a complete solution for a better information security experience, by providing the needed policies, tools and procedures for enhancing and maintaining a secure information system (Itradat et al., 2014). Furthermore, an ISMS likewise takes care of most aspects affecting an organisations information security experience; and it does so by applying the correct tools and procedures to ensure the confidentiality, the integrity and the availability of an organisations information assets (Itradat et al., 2014). (Asosheh, Hajinazari, & Khodkari, 2013), report that ISO/IEC27001 is the most widely used ISMS standard, with 163 countries using it in the year 2012. COBIT was reported as the second highest, with 160 users; and BS7799, the standard on which ISO/IEC27001 is based, reported to only have 110 users. Therefore, this research project will focus on the functioning of an ISMS, based on the ISO/IEC27001. However, other ISMS standards and guidelines will not be disregarded, when recommendations are made for the development and use of the model, which is the output of this research study.

### **2.6.4 An ISO/IEC27001 ISMS**

ISO/IEC27001 (2013) adopts the Plan-Do-Check-Act (PDCA) model, which is applied to structure the ISMS in the development and in the implementation process (Asosheh et al., 2013). The PDCA model consists of four phases, as may be seen in Figure 2.6.4.

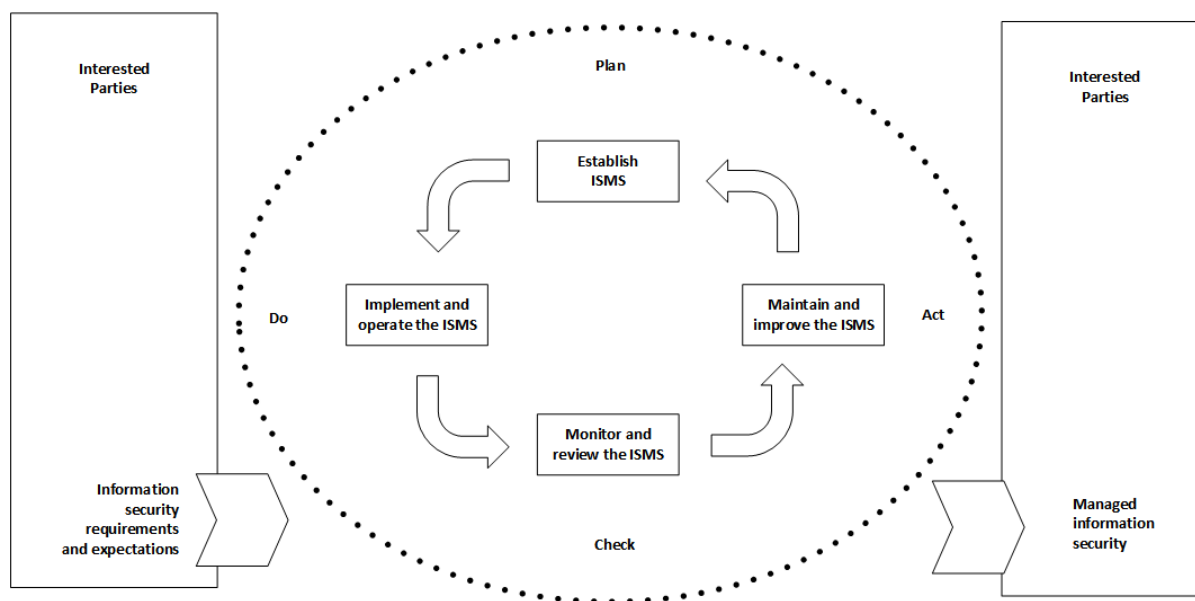


Figure 2.3: A Digram of an ISO/IEC27001 ISMS Development and Implementation Process. Adapted from (Asosheh et al., 2013)

Below is how each phase is applied in the context of ISMS development and implementation (Asosheh et al., 2013):

- The **plan** phase is required to establish the ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security, to deliver results. in accordance with an organisations overall policies and objectives;
- The **do** phase is, to implement and operate the ISMS policy, controls, processes and procedures;
- While in the **check** phase, the tasks are to check, assess and where applicable, measure process performance against ISMS policy, strategic-level information security objectives and practical experience, and report the results to a higher management level, for review; and

- Finally, in the **act** phase, those responsible for the ISMS take corrective and preventive actions, based on the results of the internal ISMS audit and management review, or other relevant information, to achieve continued improvement of the ISMS.

In addition to the four phases of the PDCA cycle, ISO/IEC27003 (2010, p. 2) also defines the following, as the five phases in the implementation of an ISMS:

- Obtaining management's approval for initiating an ISMS project;
- Defining the scope of the ISMS policy;
- Conducting an organisational analysis;
- Conducting risk assessment and risk-treatment planning; and finally
- Designing the ISMS.

The decision to adopt an ISMS is a strategic-level management decision in any organisation, not merely a technical or ICT project; and it therefore requires the buy-in from an organisation's strategic-level management (ISO/IEC27001, 2013, p. 2; IoDSA, 2009, p. 41; Calder, 2009, p. 3). Thus, it is also important that the ISMS is part of an organisation's processes and the overall management structure. The ISMS must be directly influenced by the organisation's information security objectives, its business processes and the size, and the structure of the organisation as well as its information security requirements (ISO/IEC27002, 2013, p. v; Calder, 2009, p. 3).

## 2.7 Information Security Requirements

One of the biggest challenges of designing an ISMS, is to establish the level of information security required. In order to ensure adequate protection of the informational assets and the selection of the appropriate and proportionate security controls; the design of an ISMS requires the organisation to identify its relevant

information security requirements (Asosheh et al., 2013). Information security requirements are defined as the level of information security required for each information asset of an organisation (Gerber & von Solms, 2005, 2008). Information security requirements will be discussed further in Chapter 3.

## 2.8 Conclusion

This chapter has established the outcomes of good information security governance, as discussed in section 2.4.5. Therefore, it may be concluded that the chapter has accomplished its objective, as set out in the introduction (section 2.1). In doing so, the chapter began by discussing corporate governance, its role players, and the direct/control cycle. Furthermore, the reader was introduced to a component of corporate governance, known as ICT governance. ICT governance involves the management of ICT systems and resources, as well as the risk pertaining to the use of these systems and resources. The outcomes of good information security governance, along with the output of subsequent chapters; will all contribute to deriving draft principles that will guide the development of the proposed solution presented by this research study.

However, it was realised that managing the risks of ICT systems alone cannot adequately protect the significant characteristics of an organisation's information assets. Thus, the concept of information security governance was introduced. The chapter further delved into the direct/control cycle of information security governance and the development of an ISMS based on the ISO/IEC27001 and related information security standards. Developing such an ISMS requires that organisations determine their information security requirements, which has been reported to be a challenge for most organisations. The next chapter will further discuss the information security requirements; as they relate to this research study.

# Chapter 3

## Information Security Requirements

*“Winning can be defined as the science of being totally prepared.”*

-George Allen

### 3.1 Introduction

As mentioned in section 2.7 of Chapter 2, information security requirements determine the level of information security necessary per information asset. This chapter endeavours to provide the reader with a detailed discussion of information security requirements. Thus, the objective of this chapter is twofold. Firstly, *to establish the criteria that information security best practices and standards use to define an information security requirement*. Secondly, *to report on the obtained perspective of various authors on the use and understanding of information security requirements*.

Therefore, this chapter will provide a more detailed definition of information security requirements from information security best practices and standards; as well as from literature published by various authors in the field. A section of this chapter will, therefore, specifically discuss the definition of information security requirements, as found in three well established information security best practices

and standards. Following this section, the findings from literature on information security requirements will be discussed. Finally, the author will compare two methods of establishing the information security requirements of an organisation, before concluding the chapter.

## 3.2 Defining Information Security Requirements

Although the author of an ISMS (e.g. information security best practices and standards), often recommends a basic set of information security requirements, it is necessary for an organisation to tailor the information security requirements to suit its unique characteristics (ITGI & OGC, 2008, p. 6; Broderick, 2005).

The unique information security requirements of an organisation inform information security governance, of the need for information security; and they therefore result in a holistic, top-down approach to the different mechanisms that are required to facilitate highly effective information security governance (Rasouli, Trienekens, Kusters, & Grefen, 2016).

The effective governance of information security is achieved by tailoring information security efforts to the level of information security required for each characteristic of an organisation's information assets. The level of security is specific to the characteristics of the organisation; and it is deemed as the information security requirements of the organisation (Gerber & von Solms, 2008, 2005). The information security requirements of an organisation stem from three sources, which define the criteria of information security requirements (ISO/IEC27002 & ISO/IEC27001, 2013, p. vi). These criteria are discussed in the sections that follow.

### 3.2.1 Source 1: The assessment of information security risks to the organisation

Through some form of risk analysis, the threats to information assets, vulnerabilities and the likelihood of occurrence and the potential impact are determined.

This risk analysis must take into account the overall business strategy and the information security objectives of the organisation (ISO/IEC27002, 2013, p. vi; Gerber & Von Solms, 2008).

### **3.2.2 Source 2: Principles, objectives and business requirements**

Individual organisations each have their own unique organisational principles, objectives and business requirements that facilitate the business operations of the organisation and its competitive advantages. These include how information within the organisation should be handled, processed, stored, communicated and archived. The ISMS should be tailored to support these business requirements for information (ISO/IEC27002, 2013, p vi; Gerber & Von Solms, 2008).

### **3.2.3 Source 3: Legal, statutory, regulatory and contractual requirements**

Organisations are often expected and sometimes even legally obliged to govern the security of their information assets (Amsenga, 2008). It has become imperative that organisations should be aware of legal compliance and obligations that arise from it. Obligations could demand certain information security controls, to ensure compliance. Non-compliance or ignorance of standards, regulations and legislation often result in fines or criminal penalties being enforced on an organisation, or on the management of the organisation (Gerber & von Solms, 2008; Gerber et al., 2001).

The third of the three criteria of information security requirements, stems from four obligatory derivatives (ISO/IEC27002 & ISO/IEC27001, 2013, p. vi):

- Legal- meaning laws or rules that are set and recognised by the State (in written or unwritten form) and enforced through an authority endowed with the responsibility and with the power to do so (Gerber & von Solms, 2008);

- Statutory- a written law or legislation passed by an authoritative body, such as Parliament. Statutes are therefore seen as the primary product, which will eventually result in the passing of a formal law (Gerber & von Solms, 2008);
- Regulatory- regulations that are derived from statutes and can be seen as secondary laws. These include rules or directives by any authoritative body, not necessarily the State. Regulations have the main objective of ensuring or measuring compliance with the statutes (Gerber & von Solms, 2008); and
- Contractual- requirements; which are those arising from a binding agreement between parties. These requirements must be in accordance with the law and indicate the intent of parties to meet the obligations, as agreed upon (Gerber & von Solms, 2008).

This section discussed the criteria of information security requirements, as defined by ISO/IEC27002 (2013, p. vi). It was mentioned at the end of the previous chapter, that information security requirements are necessary for an organisation to develop and implement an ISMS. It was further stated that information security requirements are a measure of how much information security an organisation needs. Information security best practices and standards provide guidance on the development and the implementation of an ISMS. Therefore, it is worthwhile to consider the definition of information security requirements, as found in information security best practices and standards. The next section of this chapter will thus review the definition of information security requirements based on information security best practices and standards.

### **3.3 Information Security Best Practices and Standards on Information Security Requirements**

Information security best practices and standards, as mentioned in section 2.5 of Chapter 2, provide a 'tried and trusted' method to achieve information security.



These best practices and standards also suggest that an organisation selects the most appropriate information security measures according to its information security needs. This section will discuss the defining criteria of information security requirements, according to three information security best practices and standards.

### **3.3.1 ISO/IEC27003:2010 Information Technology- Security Techniques- Information Security Management System Implementation Guidance**

The information security controls implemented and maintained by an organisation, whether individually or as part of an ISMS, need to meet the specific security and business objectives of the organisation. Therefore, it is essential that an organisation identifies its information security requirements (ISO/IEC27002 & ISO/IEC27001, 2013, p. vi). Furthermore, ISO/IEC27002 (2013, p. vi), suggests that the results of a risk assessment would help to guide and determine the appropriate management action and the priorities for managing information security risks, and for implementing information security controls, selected to protect against these information security risks.

However, ISO/IEC27003 (2010, p. 20) , advises on conducting an information security requirements analysis, in order to identify the information security requirements of an organisation. Furthermore, it is suggested that the objective of an information security requirements analysis is to define the relevant requirements to be supported by the ISMS, to identify information assets, and to obtain the current information security status within the organisation's information security scope. The results of an information security requirements analysis (yielding information security requirements), should provide management with a good starting point to selecting appropriate information security measures.

An information security risk assessment should be conducted after an information security requirements analysis. The main objective of the risk assessment is to take the summarised information security status and to identify vulnerable

information assets from the information security requirements analysis; and to estimate the level of information security risk and to compare this level against the information security risk evaluation criteria and information security risk acceptance criteria of the organisation (ISO/IEC27003, 2010, p. 27).

### **3.3.2 NISTIR 7621 Small Business Information Security: The Fundamentals**

The NISTIR 7621 (2009), specifies the “absolutely necessary actions that a small organisation should take to protect its information assets and networks. These can be seen as the fundamental technical information security requirements that a small organisation should have. Additionally, highly recommended practices are also included, as suggested information security requirements that a small organisation might also like to fulfil. Furthermore, an organisation can identify the protection needed by its priority information types. This is done through listing each information type and specifying Y for yes, or N for no in the columns for confidentiality, integrity and availability. However, there is no mention of the three sources of information security requirements, as established in a previous section of this chapter (NISTIR7621, 2009, pp. 2,7&B-1).

### **3.3.3 NIST SP800-53 Revision 4 (2013) Security and Privacy Controls for Federal Information Systems and Organisations**

This special publication of the NIST; specifies the minimum information security requirements for federal information systems. The information security measures specified in the NIST SP800-53 Rev4 (2013), address a diverse set of information security and privacy requirements derived from legislation, executive orders, policies, directives, regulations, standards and/or mission/business needs. Through the use of the Federal Information Processing Standards Publication (FIPS PUB) 199, organisations first determine the information security category of their information system (e.g. private, medical or financial, etc.). Following the information

security categorisation of information systems, FIPS PUB 200, is used to derive the potential level of impact of the threat to an information system. This process is ultimately the determination of the information security requirements of an organisation and the tailoring of the information security controls selected from the NIST SP800-53.

Unlike the ISO/IEC27003 (2010), the NIST SP800-53 R4 (2013) does not mention the business objectives, or the laws with which an organisation must comply (NISTSP800-53, 2013). The NIST SP800-53 Rev4 (2013, p. viii), further states that information security requirements are used by different communities within an organisation. For instance, information security requirements appear at a high level of abstraction in legislation, executive orders, directives, policies, standards, and mission as well as business needs statements. They appear in technical form in requirements used by information security engineers, system developers and system integrators. However, information security requirements can also exist in non-technical security controls that address matters, such as policy and procedures at the tactical-level and operational-level management. Information security requirements at each of these levels again exist with varying degrees of detail.

One of the objectives of this research project is to determine the criteria of an information security requirement, as specified by information security best practices and standards. This section established the sources of information security requirements and the fact that information security requirements should provide a starting point for management, as defined by the ISO/IEC27003 (2010).

The NIST SP800-53 Rev 4 (2013) reports that information security requirements nature differ, according to the community of use. However, both the NIST SP800-53 Rev (2013) and the ISO/IEC27003 (2010) standards agree that the information security requirements are eventually interpreted into information security measures that are operationally implemented.

Another objective of this research project is to determine the perspective of some authors of information security literature. This objective will be addressed in the next section of this chapter.

### 3.4 Literature on information security requirements

Previously published literature, provides the perspective and findings of authors in a particular research field. Published works have been peer-reviewed and accepted as credible sources. Therefore, this section will discuss a few findings of other authors, of works related to information security requirements.

Gerber and von Solms (2001); report that the first and foremost factor that determines which and how much information security is required, are the business requirements that dictate to what extent the CIA (confidentiality, integrity and availability) of information assets must be preserved. Furthermore, the authors state that the information security requirements of an organisation also stem from the business requirements for CIA, legal and regulatory, as well as statutory requirements and not just from the information security risks threatening the ICT infrastructure of the organisation.

Similarly, Asosheh, et. al (2013) agree that the relevant information security requirements of an organisation should be determined. This would ensure that information assets are supported by the ISMS, and that adequate and the proportionate information security measures are selected to protect the information assets. Furthermore, these authors claim that determining the required level of information security is the main challenge for the executive management of most organisations.

It was also reported that office workers are familiar with the security requirements of a filing cabinet, but not with those of an information system (Dhillon, Stahl, & Baskerville, 2009). Dhillon and Backhouse (2009), further go on to state that in the corporate world, information security is generally seen as the interests of the ICT department and consequently numerous professionals do not give adequate importance to the information security concerns of the organisation; and even if they do, they often develop over-complicated solutions.

Pertaining to the implementation of over-complicated information security solutions, Herrmann and Herrmann (2006), report that many information security approaches adopt access control and authentication methods. However, the governance of information security demands a wider view than simply attempting to secure information security assets with complicated access control systems. Thus, an organisation should undergo an information security requirements analysis, in order to identify its information security requirements.

Information security best practices and standards were intended to circumvent the need for organisations to reinvent the information security governance process. However most information security best practices and standards are found to be too generic and not encompassing of the information security requirements of the different types and sizes of organisations. Moreover, the generic nature of most information security best practices and standards frequently make them too complex for some organisations (Siponen & Willison, 2009). The next section of this chapter will briefly compare an information security risk analysis with an information security requirements analysis.

### **3.5 Information Security Risk Analysis versus Information Security Requirements Analysis**

Various methods exist to identify the information security requirements in numerous contexts. These include an information security requirements engineering process, misuse cases, common criteria (CC), threat modelling and abuse frames. However, most of these methods refer to the identification of information security requirements for the development of information systems and software systems (Myagmar, Lee, & Yurcik, 2005; Lin, Nuseibeh, Ince, Jackson, & Moffet, 2003).

The focus of this research project is, however, on information security governance. Therefore, the methods that concern the information security of information assets as a whole (not only information systems) will be considered. Thus, in this section an information security requirements analysis, which is reported to be a

more comprehensive approach to determine an organisation's information security requirements such as Gerber & Von Solms (2008); is compared with the traditional method of identifying the information security measures to be implemented by an organisation. The traditional method referred to above, is known as an information security risk analysis (Gerber & Von Solms, 2001).

### 3.5.1 Information Security Risk Analysis

An information security risk analysis is the process of identifying the information assets of an organisation, the threats to those information assets, in addition to the vulnerabilities that can be exploited by the threats. An information security risk analysis concludes with the determination of the risk level of each information asset (Whitman & Mattord, 2012, p. 140; ISO/IEC27005, 2012, p. 8; Baskerville, 1991).

Furthermore, an information security risk analysis may be undertaken in varying degrees of detail. The degree of detail depends on the criticality of the information assets, the extent of ICT vulnerabilities known and previous information security incidents involving the organisation. Thus, an organisation may initially perform a qualitative information security risk analysis and thereafter conduct a more quantitative information security risk analysis (ISO/IEC27005, 2011, p. 17).

- Qualitative information security risk analysis- utilises a scale of attributes (e.g. Low, Medium or High), to describe the impact of potential consequences and the likelihood that the consequences will occur (ISO/IEC27005, 2011, p. 17); while
- Quantitative information security risk analysis- makes use of a variety of sources to assign numerical values for the impact of consequences and the likelihood of these consequences occurring. Quantitative information security risk analysis relies on factual data from historical sources; and it becomes increasingly difficult to conduct, when this data is not available (ISO/IEC27005, 2011, p. 17).

The wide availability of the numerous information security risk analysis methods (Vorster & Labuschagne, 2005), has led to information security risk analysis becoming the most predominantly used technique for the selection of information security measures (Gerber, 2001; Baskerville & Siponen, 2002). Within qualitative and quantitative risk analysis, various methods exist to conduct an information security risk analysis, such as (Vorster & Labuschagne, 2005):

- OCTAVE (Operationally Critical Threat Assets and Vulnerability Evaluation)
- CORAS (Construct a platform for Risk Analysis of Security Critical Systems)
- ISRAM (Information Security Risk Analysis Method)
- Information Systems (IS) analysis based on a business model, among others.

Names such as OCTAVE, appeared in section 2.5; however that was a discussion of the information security best practices and standards. The above list mentions only the names of information security risk analysis methods, which can be found in the information security best practices and standards, as discussed in section 2.5 of Chapter 2. In addition to the four information security risk analysis methods listed above, it is reported that alternative information security risk analysis methods do exist. However, in comparison to traditional information security risk analysis, these alternative methods are not as widely adopted by information security professionals (Spears, 2005). This low adoption can potentially be as a result of the alternative methods being as undesirable as a traditional information security risk analysis (Baskerville & Siponen, 2002).

A traditional information security risk analysis is reported to be undesirable as the sole method for determining the appropriate information security measures, due to its focus on ICT infrastructure, rather than on the business context at large. Traditional risk analysis methods measure the potential success of an information security attack based on the identified vulnerabilities of the ICT systems. Whereas, alternative risk analysis methods consider the needs, executive

orders and operations of the organisation in addition to legal expectations. For this reason, traditional information security risk analysis was seen to present a bottom-up information security approach, contrary to the top-down information security governance approach (Fenz, Plieschnegger, & Hobel, 2016; Gerber & von Solms, 2005; Spears, 2005), as mentioned in section 2.4.4 of Chapter 2.

From the above argument, it may be concluded that information security risk analysis is not suitable as the sole method for determining the information security requirements of an organisation. Rather, a method that would incorporate the business context, as well as additional information security requirements criteria, mentioned earlier in this chapter, is necessary. Such a method will be discussed in the section below.

### **3.5.2 Information Security Requirements Analysis**

As mentioned in an earlier section of this chapter, information security requirements stem from three sources (assessing risks to the organisation, principles, objectives and business requirements, and legal, statutory, regulatory and contractual requirements). Therefore, it is only logical that a suitable method for identifying the information security requirements of an organisation should consider all three of these sources.

The fact that an information security requirements analysis requires input such as an organisation's business and information security objectives, regulatory, contractual and industry requirements, as well as management's commitment to developing the ISMS; makes an information security requirements analysis a more desirable method for identifying the information security requirements of an organisation (ISO/IEC27003, 2010, p. 22). Organisations vary in size and in their objectives (both business and information security). Therefore, it is not possible to have a single method, which will suit every organisation. An information security requirements analysis considers the scalability needs and the objectives of the organisation. Thus, the unique nature of the organisation is reflected in the identified information security requirements (Gerber & Von Solms, 2005).



The information security requirements to be determined through an information security requirements analysis are inclusive of the criteria of an information security requirement. In simpler terms, an information security requirements analysis has the capability to determine the amount of CIA (confidentiality, integrity and availability), as that is required for each information asset of an organisation (Gerber & Von Solms, 2008). A number of information security requirements analysis methods exist, such as the following (Herrmann & Herrmann, 2006):

- MOAT (Methodically Organised Argument Trees)
- RDR (Risk Data Reporting approach)
- HAZOP (Hazard and Operability Analysis)

However, most of these methods are based on software engineering methods; and they therefore do not necessarily apply to all organisations as not all organisations are software engineering firms (Herrmann & Herrmann, 2006). Furthermore, the workers of an organisation may be familiar with the security requirements of a filing cabinet, but not necessarily those of an information system. For this reason, information security is generally cast upon the ICT department (Dhillon et al., 2009). Another reason for this could be that in most cases, the strategic-level management of the organisation does not understand the required level of information security (Asosheh et al., 2013).

It was mentioned in a previous chapter that the strategic-level management of an organisation is accountable for information security governance. Furthermore, it was mentioned in this chapter too, that the results of an information security requirements analysis (information security requirements), should provide management with a starting point, and eventually lead to the selection of the most suitable information security measures.

Information security measures are generally selected and implemented at the operational management level (as seen in Chapter 2). Also mentioned in Chapter 2, was the fact that the implemented information security measures should stem

from the directives issued by the strategic level management of an organisation. The communication of information security requirements through the management levels relies on intra-tier and inter-tier communications of the management levels (NISTSP800-53, 2013, p. 8).

D'Arcy, Herath and Shoss (2014), report that the proper communication of information security requirements is crucial, as confusing information security requirements can lead to non-compliance. Research has however, challenged the current methods of translating high-level information security requirements into information security controls (Thalmann, Bachlechner, Demetz, & Maier, 2012; Lakshminarayanan, Liu, Chen, Easterbrook, & Perry, 2006).

Likewise, the aim of information security governance is to align the information security of the organisation with the governance of the organisation. Therefore, information security cannot be seen apart from the business strategy. For this reason, the translation of high-level information security requirements into operational-level information security measures, needs to be traceable and testable (Manhart & Thalmann, 2013). It is, however, reported that the implementation of such a system tends to be complex; and it commonly requires expensive information security expertise (Herrmann & Herrmann, 2006).

### **3.6 Conclusion**

This chapter has expanded on the concept of information security requirements, as introduced in section 2.7 of Chapter 2. Furthermore, a detailed definition of information security requirements was presented. This detailed definition included the three sources of information security requirements, as seen in section 3.2.

Moreover, it was established that information security best practices and standards offer varying criteria to define information security requirements (see section 3.3). However, for this research study, the three sources of information security requirements are considered as being the criteria of an information security requirement.

It was also established in this chapter that several authors deem information security requirements to be important. This was supported by the fact that information security requirements provide a starting point in selecting the information security controls within an organisation.

Finally, the author presented an information security requirements analysis as an improved method to establish the information security requirements of an organisation. However, the information security requirements analysis was reported to be a supporting method, and not an alternative to an information security risk analysis. According to the above summary, it may, therefore be conclude that this chapter has accomplished both of its objectives, as stated in section 3.1. The findings of this chapter, in conjunction with the findings of Chapter 2 and Chapter 4, will contribute to draft principles, which will guide the development of the solution proposed by this research study. The draft principles will be discussed in section 7.2 of Chapter 7.

It was also reported in this chapter that establishing the information security requirements of an organisation can be complex and it often requires information security expertise. Most small, medium and micro enterprises (SMMEs) generally cannot afford such expertise (Devos et al., 2012). Chapter 4, will present a discussion on SMMEs.

# Chapter 4

## Information Security Governance in Small, Medium and Micro Enterprises

*“Research is formalised curiosity. It is poking and prying with a purpose.” -Zora Neale Hurston*

### 4.1 Introduction

The previous chapter concluded that most SMMEs cannot afford the information security expertise often required to establish the information security requirements of an organisation. Devos et al. (2012), agree with this statement; as they claim that the size of an organisation is reported to be a factor in its ability to employ individuals with specialised skills. Furthermore, these authors claim that the smaller the organisation, the less able it is to afford to employ individuals with specialised skills. Congruently, Upfold (2005, p. 46), alleges that SMMEs do not have the resources to implement complex information security strategies (Upfold, 2005, p. 46).

Thus, in accordance with the primary objective of this research study; this chapter seeks *to determine the core elements of an artefact developed*

*for SMMEs.* These core elements will be used in a later chapter (Chapter 7), to develop a less complex method for SA SMMEs to establish their information security requirements.

This chapter begins by reviewing the various global definitions of SMMEs, before defining the criteria used to categorise an organisation, as an SMME in SA. Further sections discuss the importance of SMMEs to the economy, the constraints and the characteristics of SMMEs as well as corporate governance from an SMME perspective. This chapter also gives an overview of how information security governance is conducted in SMMEs and the use of information security best practices in SMMEs. A final section presents the core elements of an artefact developed for SMMEs, before the chapter is concluded.

## 4.2 Defining Small, Medium and Micro Enterprises

Koornhof (2009, p. 12), claims that historically all business organisations were SMMEs and therefore it was not necessary to differentiate between the sizes of organisations. However, a shift from the owner-manager (and CEO) corporate governance structure, common to SMMEs brought about the need to categorise organisations. Organisations, where the owner-manager corporate governance structure exists, are reported frequently to have the same individual, who is the owner of the organisation also fulfilling all the management roles within the organisation. Moreover, even in the categorisation of organisations, all organisations cannot be viewed through the same lens. Assuming that all SMMEs will eventually morph into large organisations, is not an accurate enough assumption to treat SMMEs as miniature versions of large organisations. Therefore, it is argued that the unique characteristics of SMMEs warrant a definition specific to this type of organisation (Devos et al., 2012).

However, even as SMMEs account for more than 90 per cent of all business organisations worldwide (Ayat et al., 2011), it is reported that no universally

accepted formal definition exists to define organisations as SMMEs (Devos et al., 2012). The definition of SMMEs, is reported to vary, based on a number of factors, such as geographical location and country specific laws (Smit et al., 2012; Ayat et al., 2011).

Furthermore, it is reported that some authors attempt to define SMMEs according to quantitative values such as size and capital assets. However, size as a defining parameter suffers from a lack of universal applicability. This is as the size of an organisation could refer to any of the following: number of employees, annual turnover, and economic sector of the organisation, ownership of the organisation and the value of fixed assets owned by the organisation (Abor & Adjasi, 2007; Levy, 2009).

An example of the above, would be that defining an organisation as small depends on the criteria for what qualifies as small (Boubala, 2010). Thus, other authors use the skill level of the labour force employed by the organisation and the annual turnover level of the organisation, as the defining characteristics. Some definitions of SMMEs, are based on qualitative characteristics, such as the legal status and the method of production used by an organisation. Therefore, while some countries use only qualitative parameters to define SMMEs; and others use only quantitative parameters, others choose to use a combination of both (Boubala, 2010; Ayat et al., 2011).

The European Commission (EC), applies a combination of quantitative and qualitative parameters in defining SMMEs. The EC uses parameters, such as annual turnover (not exceeding 50 million Euros), annual gross profit (not exceeding 43 million Euros), and the number of employees (fewer than 250 persons). The general definition of SMMEs by the EC, is similar to the definition of SA SMMEs, as seen in the National Small Business Act (NSBA) of 1996 (Devos et al., 2012; Burns, Davies, & Davies, 2006; The President's Office, 1996).

### 4.3 SMMEs in South Africa

As stated in the previous section, the SA definition of SMMEs is similar to that of the EC; and it takes both qualitative and quantitative parameters into account. However, the SA definition of SMMEs considers the total value of gross assets of the organisation, unlike the annual gross profit in the EC definition (Boubala, 2010). This act, defines an SMME as a separate and distinct business enterprise, which includes co-operative enterprises and non-governmental enterprises. Furthermore, the operations of the enterprise can be carried out in any sector, or subsector of the economy. Additionally, the enterprise and its branches, or its subsidiaries, must be managed by one or more owner(s) (The President's Office, 1996; Boubala, 2010). Furthermore, the SMME sector in SA can be divided into three categories, as listed below:

- Micro enterprises;
- Small enterprises; and
- Medium enterprises.

Micro enterprises, being the smallest of the categories can further be divided into survivalist and very small enterprises. Organisations considered as survivalist enterprises, operate in the informal sector; and they are created out of necessity by individuals who could not get alternative job opportunities. Very small enterprises, on the other hand, operate in the formal economy; and they have access to modern technology (Boubala, 2010, p. 27).

Below, is a summary of the NSBA Schedule's (1996) description and differentiation characteristics of SMMEs. The NSBA Schedule (1996) depicts the three categories of SMMEs, with an expansion of the micro category, to include very small enterprises as a separate category.

The parameters for differentiating between the different categories of SMMEs is the number of full-time paid employees, the annual turnover of the organisation,

and the gross asset value of the organisation. The maximum values vary, according to the economic sector to which the SMME belongs (construction, manufacturing, technology, etc, not shown in Table 4.1) (The President's Office, 1996). Table 4.1, only shows the average values; and it is a summary of the different SMME categories. The full NSBA Schedule is attached as Appendix A.

<b>Size or class (Categories)</b>	<b>Total full-time equivalent paid employees</b>	<b>Total annual turnover (million)</b>	<b>Total gross asset value (fixed property excluded) In R (million)</b>
Micro	5	0.15	0.1
Very small	20	5	1.8
Small	50	25	4.5
Medium	200	50	18

Table 4.1: Summary of NSBA Schedule

(The President's Office, 1996)

## 4.4 The Importance of SMMEs to the Economy

It is widely agreed that SMMEs are essential to the economy of any nation; and more specifically, they are central to the inclusion of developing countries in the global economy (UNIDO, 2002, p. 3; Koornhof, 2009, p. 17; Ongori & Migiro, 2010; Smit & Watkins, 2012; Valli et al., 2014; Devos, et al., 2011). Although the economic contribution of SMMEs is largely seen in developing countries, SMMEs play a major role in developed countries too. It is reported that SMMEs in first world countries, like the United States of America and the United Kingdom, contribute about one third of industrial employment. While in third world countries, such as South Africa, SMMEs dominate by economically contributing to economic growth, job creation and poverty alleviation (Smit et al., 2012; Ongori & Migiro, 2010).

Thus, it is reported that the SMMEs in existence in third world countries, ex-



ceed the large organisations in these countries. More so, SMMEs in third world countries, are reported to perform more labour-intensive processes than most large organisations. These labour-intensive processes require larger work forces; therefore, SMMEs employ more individuals, thereby decreasing the unemployment rate, and ultimately distributing income and alleviating poverty (UNIDO, 2002, p. 3; Ngura, Kimwele & Rotich, 2015; Ongori & Migiro, 2010; Smit & Watkins, 2012). Furthermore, SMMEs do not only create new employment, but they are also seen as absorbents of previously employed individuals who, have been retrenched from - either their jobs in the private sector - or in the public sector (Smit et al., 2012).

In a bid to curb a 25 per cent unemployment rate, the SA government endeavours to create an environment, in which SMMEs can thrive, as part of the National Development Plan (NDP) 2030 (BER, 2016, p. 5; Smit & Watkins, 2012). The NDP 2030, is a strategic blue-print of the SA government's strategy to alleviate poverty and to reduce inequality in SA by the year 2030. Thus, the previously mentioned benefits of the SMME sector (distributing income, poverty alleviation and creating employment), make SMMEs the trusted vehicle, which will lead any economy to salvation - and SA to achieving its NDP 2030 goal (Dube et al., 2011).

Already, SMMEs in SA are reported to contribute over 40 per cent to the gross domestic product (GDP) of the SA economy (van Niekerk & Labuschagne, 2006; BER, 2016, p. 6). Excitingly, in the year 2015, there were reportedly 2 251 821 SA SMMEs in existence (BER, 2016, p. 16). However, research studies have shown that there are more SMME closures than expansions (Smit & Watkins, 2012). Alarmingly, van Niekerk and Labuschagne (2006), estimated that SMMEs in SA were failing at a rate of 80 per cent. The high failure rate of SMMEs in South Africa is attributed to a number of constraints that challenge the success of SMMEs in SA and on a global scale (Smit & Watkins, 2012; BER, 2016, p. 10; van Niekerk & Labuschagne, 2006).

## 4.5 Constraints to the Success of SMMEs

As mentioned in section 4.4, SMMEs in SA are plagued with constraints that challenge their success and ultimately result in the high failure rate of SA SMMEs. Specifically, it is reported that SMMEs in SA typically survive for less than three and a half years on average (BER, 2016, p. 10). The low survival rate of SMMEs, especially those in third world countries, such as SA, is attributed to constraints, such as limited financial and human resources, a lack of skilled labour force (expertise) and a lack of managerial (corporate governance) skills (Ongori & Migiro, 2010; Dube, 2011; Biekpe, 2007). In addition to the above, SMMEs in South Africa experience constraints, such as poor infrastructure, low levels of research and development, high levels of crime, onerous laws and inefficient government bureaucracy, in addition to a lack of access to markets (BER, 2016, p. 10).

In the section above, a number of constraints to the success of SMMEs were listed, as obtained from various literary sources. However, Table 4.2, below, is a summary of the constraints to the success of SMMEs. These constraints also restrain the use of information security best practices and standards by these enterprises. How the constraints in Table 4.2 affect the use of information security best practices and standards in SMMEs, is discussed in section 4.9.

<b>Constraints to the success of SMMEs</b>
Limited finance
Limited human resources
Lack of expertise
Lack of governance
Poor infrastructure

Table 4.2: A table of the constraints to the success of SMMEs

Although SMMEs in third-world countries struggle to survive, due to the constraints mentioned above, these organisations have unique characteristics. The unique characteristics of SMMEs, give them a competitive edge over large organisations; and they make SMMEs a valuable asset to developing countries (Levy, 2009; Dube, 2011).

## 4.6 The Characteristics of SMMEs

As mentioned in the previous section of this chapter, SMMEs in third world countries are faced with constraints that challenge their survival. However, as seen in the list below, a number of unique abilities still allow SMMEs to be a viable salvation for the economies of many developing countries (Levy, 2009; Dube, 2011). These characteristics include the proviso that SMMEs:

- Are innovative organisations (Levy, 2009);
- Are flexible in their organisational structure (Levy, 2009);
- Are able to respond quickly to customer demands (Levy, 2009);
- Can generate new employment (Koornhof, 2009, p. 17);
- Can keep larger organisations competitive (Koornhof, 2009, p. 17); and
- Can constantly evolve (ACCA, 2015, p. 4).

Table 4.3, below, is a summary of the characteristics of SMMEs. To form the characteristics, the unique abilities of SMMEs were summarised and combined with the parameters for an organisation to be classified as an SMME, as defined by the NSBA, to form a table of the characteristics of SMMEs. The parameters used, include the annual turnover of the organisation, the maximum number of employees of the organisation and the total value of the assets owned by the organisation. Summarising the unique abilities of SMMEs, entailed combining similar abilities, such as being innovate and quick to respond to customer demands; flexible organisational structure with generating new employment; and finally that SMMEs have the ability to constantly evolve, keeping larger organisations competitive.

Characteristics of SMMEs
Flexible organisational structure
Constantly evolving
Respond quickly to customer demands
200 or less employees
50 million rand or less revenue
18 million rand or less assets

Table 4.3: A table of the characteristics of SMMEs

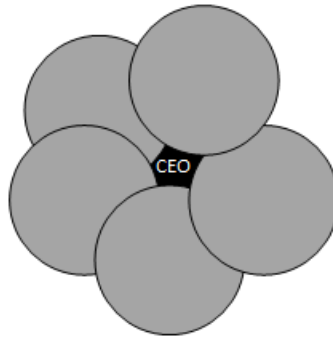
Related to the ability of SMMEs to constantly evolve, the Association of Chartered Certified Accountants (ACCA), reports that the corporate governance management structure of an organisation, must evolve, as the organisation evolves (ACCA, 2015, p. 7). It is argued that this corporate governance management structure is what differentiates large organisations from SMMEs (Beaver & Prince, 2004).

## 4.7 The Corporate Governance of SMMEs

As mentioned in the previous section, a number of constraints challenge the survival of SMMEs. One constraint, the lack of managerial skills (a proper corporate governance structure), was additionally reported to be the differentiating factor between SMMEs and large organisations (Ongori & Migiro, 2010; van Niekerk & Labuschagne, 2006; Beaver & Prince, 2004). True to this argument, Abor and Biekpe (2007), claim that SMMEs are typically not associated with corporate governance; as corporate governance is seen to be a practice for large organisations. Furthermore, the authors report that in large organisations, there is a pronounced separation of management and ownership. However, in SMMEs, it is common that there is only one [corporate governance] management level. Sometimes, the levels of management increase, as the organisation matures (Hankinson, Bartlett, & Ducheneaut, 1997).

In the one management-level configuration, the owner-manager of the organisation, is central to the web and holds all decision-making power within the organisa-

tion. This is known as an owner-manager, or CEO-centric management structure; and it is represented by Figure 4.1, below (Levy, 2009; Hankinson et al., 1997).



**Model 2: CEO/Owner Centric**

Figure 4.1: Flexible and Informal Organisational Structure. Adapted from Hankinson et al.,(1997)

Similarly, a study conducted by Beaver and Prince (2004), found that SMMEs in the United Kingdom (UK), were found to have a similar management structure, in which the owner of the organisation is the key decision-maker. Therefore, the key decision-maker cannot be separated from any of the motivations and actions for decisions made within the organisation, as can be seen in Figure 4.2.

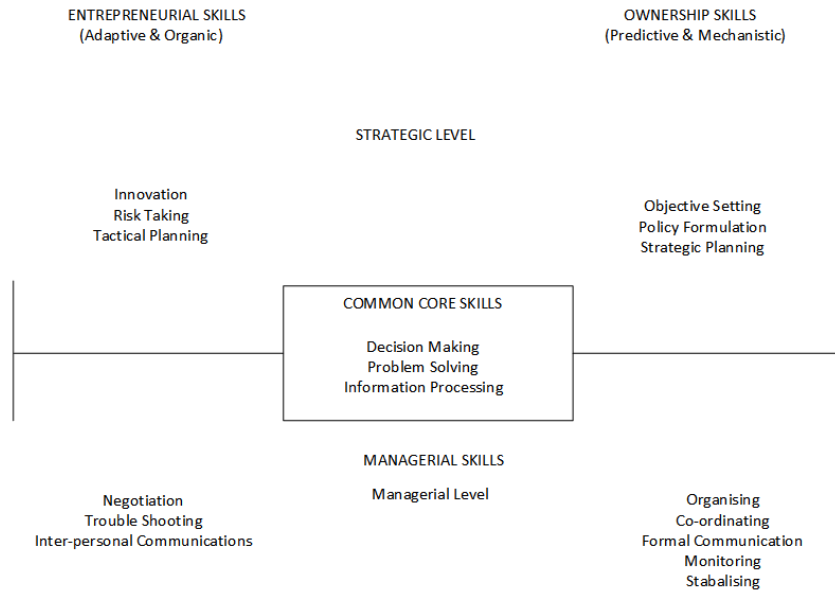
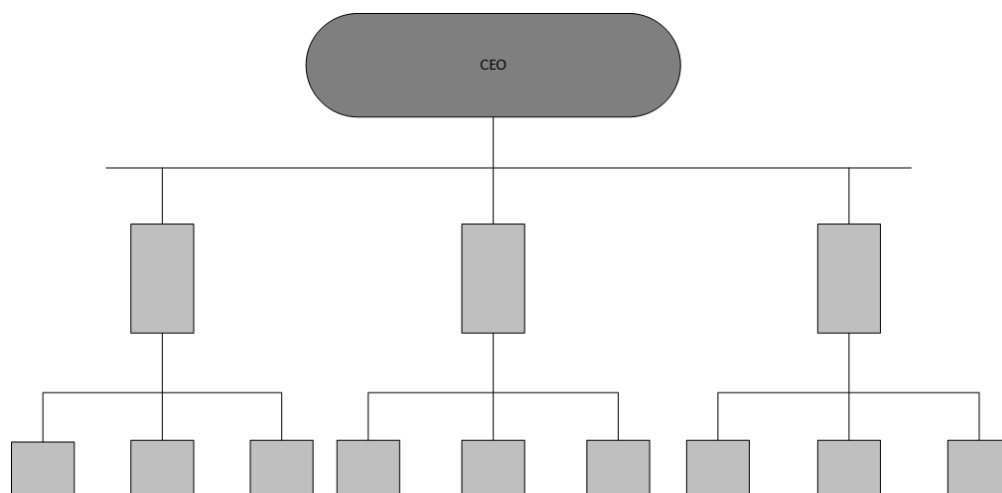


Figure 4.2: The SMME Organisational Structure. Adapted from Beaver and Prince (2004)

Thus, it may be concluded that the typical management structure of SMMEs, is central to a single individual, as the owner-manager or CEO and the sole decision-maker.

Unlike SMMEs, where corporate governance is about improving business efficiency and performance, corporate governance in large organisations is concerned with monitoring management actions (ACCA, 2015, p. 4). Therefore, large organisations tend to have a more differentiated management structure, in which the managers report to a manager of senior rank compared to them, as with the corporate governance discussion in Chapter 2 (Hankinson et al., 1997). Figure 4.3, below, is a representation of the differentiated and hierarchical management levels similar to Figure 2.2.1.



**Model 1: Differentiated Management**

Figure 4.3: Structured and Hierarchical Organisational Structure. Adapted from Hankinson, Barlett and Ducheneaut (1997)

Banham and He (2010), claim that the overlap between ownership and management in SMMEs creates complexity in corporate governance relations. This complexity includes barriers in the development of better strategies and taking more innovative approaches. Thus, Dube (2011) suggests that with the growth of organisations, there is a need to introduce professional management and governance practices. In this regard, Abor and Biekpe (2007), argued that similar corporate governance best practices and standards that apply to stock-exchange listed organisations, should also apply to SMMEs.

However, most established corporate governance best practices and standards are developed mainly for the use of large, stock exchange listed organisations (Dhillon et al., 2008; ACCA, 2015, p. 3); whereas SMMEs, have unique characteristics and constraints (as discussed in sections 4.6 and 4.5, respectively), which set them apart from large organisations (Devos et al., 2012). Therefore, most established corporate governance best practices and standards are not suitable to the SMME environment, as they do not cater for the unique characteristics and

constraints of SMMEs (Dhillon et al., 2008; ACCA, 2015, p. 3). Studies have discovered that most corporate governance approaches are also developed mainly for the use of large organisations and are therefore also not suitable for SMMEs (Dhillon et al., 2009; Van Niekerk & Labuschagne, 2006).

As this research study is concerned with information security governance as a component of ICT governance, further discussions will be about information security governance in SMMEs.

## 4.8 Information Security Governance in SMMEs

Before discussing the issues related to the implementation of well-established information security approaches, best practices and standards in SMMEs, it is necessary to establish how information assets are protected in SMMEs. For this reason, this section will discuss information security governance in SMMEs.

Information security attacks are not only relevant to large organisations, but also to SMMEs (Bhattacharya, 2008, p. 6). However, a study by Kankahalli, Tou, Tan and Wei (2003) found that most SMMEs implement fewer information security measures than do large organisations. Furthermore, Coertze and von Solms (2013) report that many SMMEs do not comply with information security governance principles, because of volatile economic challenges, such as war, recession, poverty and a lack of resources and expertise.

Contrary to these findings, Valli, Martinus and Johnstone (2014), conducted a study that found that most SMME owner-managers do not comply with information security governance principles as they do not believe that their organisations are under attack. The results of the study concluded that 75 per cent of the respondents do not believe that their organisations are the targets of information security attacks. A further 59 per cent of the respondents are of the opinion that their organisations do not possess any information assets, which could be valuable to attackers. However, there have been studies, which have concluded that SMMEs are, in fact, a growing target of information security attacks (Feagin, 2015).



Interestingly, a survey on the targets of information security attacks, which occurred in the year 2012, showed that the largest growth in information security attack targets [in particular cybersecurity attacks] were SMMEs. An estimated 31 per cent of all information security attacks which occurred in 2012 were believed to be targeted at SMMEs (Valli et al., 2014).

SMMEs, as mentioned in a previous section, struggle in aspects, such as finance and access to markets, eventually leading to their premature failure (BER, 2016, p. 10). Therefore, it is essential for SMMEs to address the issue of information security and privacy risks; as they could potentially disrupt the business continuity; and cause monetary, reputational and other losses to the organisation. These losses could ultimately cost the organisation its success (ENISA, 2016, p. 27).

The success, efficiency and use of resources, as mentioned in Chapter 2, are the responsibility of SMME corporate governance (ACCA, 2015, p. 4). Although there are benefits of using ICT for business strategy, research shows that most SMME owner-managers do not use ICT, as a link to business strategy (Ngura et al., 2015). Extending this sentiment to information security, most SMME owner-managers are reported to not be supportive of information security due to both financial and time constraints (Ngura et al., 2015; Goucher, 2011; Dojkovski, Lichtenstein, & Warren, 2007).

Thus, the information security efforts of an SMME become a balancing act, in which the actions of any one individual can tip the scales. Risk management too becomes more of a reactive measure, rather than a proactive one (Upfold, 2005, p. 46). Risk management responsibility in SMMEs usually resides with the owner-manager (Smit et al., 2012). This is, however, not the ideal situation; as Krishna (2010), reports that SMME owner-managers generally have a weak understanding of information security management.

However, as discussed in section 4.7, the use of established information security approaches, best practices and standards, so easily becomes “a road that is too long for an SMME to travel” (Sánchez, Ruiz, Fernández-Medina, & Piattini, 2010). This will be discussed further in the next section of this chapter.

## 4.9 Information Security Best Practices and Standards in SMMEs

The implementation and availability of an ISMS has become a critical component in the success of SMMEs. The success of the ISMS depends on the adaptation of an ISMS standard to the unique characteristics and availability of resources of an SMME (Sánchez, Villafranca, Fernández-Medina, & Piattini, 2009). However, most SMMEs never reach a fully implemented standard; and they revert to ad hoc implementations of information security measures. This is mainly due to the complex information security requirements prescribed by some well-established ISMS best practices and standards, such as the NIST SP800-53 R4 (2013) (Mijnhardt, Baars, & Spruit, 2016).

The problem experienced by most SMMEs in implementing information security best practices and standards is two-fold, as discussed in section 4.7. Firstly, information security best practices and standards have complex requirements that cannot be met by the limited financial resources and expertise of most SMMEs (Clarke, 2015; Coertze & Von Solms, 2013; Beranek, 2011; Barlette & Fomin, 2010; Ernest Chang & Ho, 2006). Secondly, information security best practices and standards are developed mainly with large organisations in mind (Hutchinson, Armitt, & Edwards-Lear, 2014). Where information security best practices and standards are developed for implementation in SMMEs, they are usually internationally endorsed; and they are not aligned with local legislative and regulatory requirements (Van Niekerk & Labuschagne, 2006).

In addition to these requirements, SMMEs experience the challenges of aligning the information security best practices and standards with their unique characteristics. The unique characteristics of SMMEs include their flexibility to dynamically adjust to markets and change the way that the organisation does business (Tawileh, Hilton, & McIntosh, 2007). Information security best practices and standards frequently do not take into account how SMMEs conduct business or the corporate objectives of SMMEs. Therefore, most well-established information security best

practices and standards are sometimes seen as a hindrance to the business of an SMME, as they do not include how specific information security controls can be aligned to the corporate objectives (Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011; Barlette & Fomin, 2008). Thus the owner-managers of SMMEs prefer to manage information security as best they know (Njenga & Jordaan, 2016).

As noted in a previous section of this chapter, SMMEs find challenges in applying corporate governance best practices and standards. Similarly, SMMEs have difficulty in applying information security best practices and standards for the same reasons. To address this problem, in particular, the implementation of information security best practices and standards in SMMEs, it is necessary to adapt methods to the unique characteristics of SMMEs. Information security risk analysis methods should be adapted to the unique characteristics of SMMEs to assist them in establishing their required level of information security and the most suitable information security measures (Sánchez et al., 2010; Barlette & Fomin, 2008). Furthermore, the information security controls identified must be well aligned with the corporate objectives of the organisation (Barlette & Fomin, 2008).

The ACCA (2015, p. 4) suggest characteristics and features that a research artefact suitable for all types of organisations, in particular SMMEs, should possess. According to ACCA (2015, p. 4), any research artefact developed for SMMEs should possess the characteristics, as can be seen in Table 4.4.

<b>Characteristics of an SMME Artefact</b>
Fit for purpose (appropriate for organisation size and maturity)
Clarity on decision making and risk controls
Promote understanding of roles and responsibilities
Show a clear communication of strategy from the board to management and staff
Suggest appropriate internal controls related to risks
Enable boards to have insight on management decision about risk management

Table 4.4: The characteristics of an artefact developed for SMMEs.

## 4.10 The Core Elements of an Artefact for SMMEs

The European Union Agency for Network and Information Security (ENISA, 2016) suggests that SMMEs could benefit from a more guided approach to bridge the gap between their perception of information security risk and the legal provisions. Legal provisions in this context are reported to include legislation, which places the liability on the enterprise.

Furthermore, it is reported that such guidance should be based on information security best practices and multidisciplinary approaches, which would allow SMMEs to self evaluate the effectiveness of their information security. Therefore, SMMEs effectively could benefit from a more guided approach that they can use to determine their information security requirements, based on information security best practices and other guiding standards (ENISA, 2016, p. 6).

Furthermore, one of the secondary research objectives of this research study was to determine the core elements of an artefact designed for SMMEs, as seen in Figure 1.8.1 in Chapter 1. The purpose of the artefact developed by this research study, would be to offer SA SMMEs a more guided approach to determine their information security requirements, as suggested by ENISA (2016, p. 16).

Therefore, to determine the core elements of an artefact for SMMEs, guidance was sought from various multidisciplinary literary sources. These sources include the National Small Business Act of 1996 (The President's Office, 1996), information security for SMMEs white papers (ENISA, 2016), and other literature originating from the business management field of study.

The discoveries from literature, which culminated in determining the core elements, were discussed in section 4.3 to section 4.9 above.

Table 4.5, below, is a combination of Tables 4.2, 4.3 and 4.4, as seen earlier in sections 4.5, 4.6 and 4.9 of this chapter. Each of the items in Table 4.5 is labelled alphabetically, for ease of discussion on the role the item played in determining the core elements, which will be discussed later in this section.

Characteristics of SMMEs	Constraints to	Characteristics of SMME Artefact
(a) Flexible organisational structure	(g) Limited finance	(l) Fit for purpose (appropriate for organisation size and maturity)
(b) Constantly evolving	(h) Limited human resources	(m) Clarity on decision making and risk controls
(c) Respond quickly to customer demands	(i) Lack of expertise	(n) Promote understanding of roles and responsibilities
(d) 200 or less employees	(j) Lack of governance	(o) Show a clear communication of strategy from the board to management and staff
(e) 50 million rand or less revenue	(k) Poor infrastructure	(p) Suggest appropriate internal controls related to risks
(f) 18 million rand or less assets		(q) Enable boards to have insight on management decision about risk management

Table 4.5: A summary of the characteristics and constraints of SMMEs.

The identified characteristics and constraints, as seen in Table 4.5 above, were combined to formulate six core elements, which contributed to the seven draft principles that guided the model output by this research study (see section 7.2 of Chapter 7). These six core elements, were confirmed in the SA SMME sector - through triangulation - by conducting a survey, as discussed in Chapter 6.

The six core elements referred to above, are as seen below:

1. **Scalability**- As reported in section 4.6, SMMEs are flexible in their organisational structure (a) and they are constantly evolving (b) (Levy, 2009; ACCA, 2015, p. 4). Therefore the draft principles (see section 7.2 of Chapter 7) must ensure that developed artefact should be dynamic, able to adapt to the ever changing needs and structure of an SMME. Thus, the draft prin-

ciples include the need for the artefact to be adaptable to most common SMME management structures, as seen in section 7.5.

2. **Simplicity**- As SMMEs are reported to respond quickly to customer demands (c) (Levy, 2009). The draft principles must ensure that the artefact should not be complex in a manner, which hinders the ability of the organisation to continue with its business operations. As discovered from literature and proven through a survey, SA SMMEs lack information security expertise (i), thereby, increasing the need for the artefact to be simple enough to implement without vast expert knowledge, or unnecessarily large workforces (d).
3. **Feasibility**- According to the NSBA (1996) and the BER (BER, 2016, p. 10), SMMEs, especially those in South Africa, have limited human resources (h), limited financial resources (e and g) and poor infrastructure (f and k). Therefore, the draft principles should ensure that the developed artefact is not too resource intensive to implement.
4. **Utility**- Like most solutions, the draft principles should ensure that the developed artefact would be fit for its purpose. Along with scalability, the artefact must be appropriate for the size of the organisation and the level of maturity of that enterprise (l) (ACCA, 2015, p. 4).
5. **Transparency**- Among the characteristics of an artefact developed for SMMEs, the ACCA (2015, p. 4), lists clarity on decision making (m), understanding of roles and responsibilities (n), as well as showing a clear communication from executive management (o), as the necessary characteristics to be possessed by an artefact developed for SMMEs. Therefore, the draft principles must ensure that the developed artefact be cognisant of and transparent in showing the process of governance within the SMME (j).
6. **Risk control**- characteristic requirements of an artefact for SMMEs, include clarity on how decisions are made, concerning risk controls suggesting appropriate internal controls related to risks (p) and enabling executive manage-

ment to have insight on decisions about risk management (q) (ACCA, 2015, p. 4). Thus, the draft principles must ensure that the developed artefact should show a clear path on the identification of information security risk and the selection of information security controls.

The relationship between each of the core elements as seen in the above discussion can thus be summarised in one table, as seen below, in Table 4.6.

Core Element	Table 4.5 Constraints/Characteristics
Scalability	a and b
Simplicity	c,d and i
Feasibility	e, f, g, h and k
Utility	l
Transparency	j, m, n and o
Risk control	p and q

Table 4.6: A table of the relationship of the constraints and characteristics with the core elements.

## 4.11 Conclusion

The objective of this chapter, as stated in section 4.1, was to establish the core elements of an artefact developed for SMMEs. These core elements will later partially contribute to draft principles, which will be used to guide the development of the proposed solution of this research study. Thus, the chapter began by reviewing the definition of SMMEs, globally. Following this global definition, the author presented the criteria used to classify SA organisations as SMMEs.

Further, this chapter investigated the importance of SMMEs to the economy of countries and various constraints to the success of SMMEs. Also presented in this chapter were the characteristics of SMMEs, corporate governance in SMMEs and information security best practices and standards in SMMEs. Together, these discussions, along with other literature, culminated in the establishment of the six core elements of an artefact developed for SMMEs (see section 4.10).

*CHAPTER 4. INFORMATION SECURITY GOVERNANCE IN SMALL, MEDIUM AND MICRO*

The following chapter (Chapter 5), will discuss the research design that was followed throughout this research study.



# Chapter 5

## The Research Design

*"To fail to plan, is to plan to fail."*- Robert Wobbolding

### 5.1 Introduction

Olivier (2009, p. 1) defines academic research as following a systematic approach in discovering facts. Although the facts discovered in academic research are not required to be original, they can be used to identify a new or improved solution to an identified problem. Similarly, previously published literature was reviewed in the preceding chapters of this dissertation. The purpose of reviewing previously published literature was to present the facts and the identified research problem. The proposed solution to the discovered research problem will be discussed later, in Chapter 7.

The objective of this chapter is *to discuss the systematic approach that was used throughout this research study*. This systematic approach was followed in discovering facts, and in presenting a potential solution to the research problem, as seen in section 1.6.1 of Chapter 1.

The rest of this chapter is divided into five distinct sections. Firstly, the research design section, which discusses the systematic approach used throughout this research study. Secondly, a section on the research design in context will dis-

cuss how the researcher followed the systematic approach, in the context of this research study. The third section of the chapter will discuss the various research methods that were used by the researcher in conducting this research project. A fourth section of the chapter briefly mentions the limitations which affected the research study. Finally, in the concluding section, the researcher will review the discussions of this chapter, to ensure that the purpose of the chapter has been met.

## 5.2 The Research Design

It is reported that the major difference between academic works (such as this research study) and consultancy contributions is that academic works are scientific (Olivier, 2009, p. 109). Scientific works should adhere to four conditions. Firstly, the work deals with a specific research object (the issue to be investigated); it must be defined, so that others can identify it as that which is being studied. In the context of this research study, the research object is identified as information security requirements in SA SMMEs. Secondly, the research must contribute to the body of knowledge, either through new knowledge, or an improvement of the existing knowledge. Thus, the researcher in this research study, reviewed previously existing knowledge in literature; and subsequently developed a solution with a different perspective to that which is currently known. This solution is discussed in Chapter 7 of this dissertation. Thirdly, the work must be useful to others. Particularly, the solution developed in this research study, is intended to be useful to SA SMMEs. Fourth and finally, the work must provide the elements required to verify or disprove the hypothesis it presents (Eco, 2015, pp. 27-30).

Therefore, draft principles for the development of the solution were derived from the findings of Chapters 2, 3 and 4. The outcomes of good information security governance established in Chapter 2, the criteria of an information security requirement, and the core elements of an artefact developed for SMMEs established in Chapter 4; were combined to derive draft principles that guided the development of the proposed solution. Furthermore, the findings of the survey, as discussed in Chapter 6, confirmed the validity of the draft principles for SA SMMEs. The same

draft principles that were used to guide the design of the solution (see Chapter 7), were used to evaluate the solution in Chapter 8. Furthermore, for scientific works to be verifiable, the research study should be repeatable with similar results obtained, when the same parameters as those in the original study are used. Therefore, the research design of a study is important; as it explains the process followed by a researcher to arrive at a solution or a conclusion pertaining to the research problem (Olivier, 2009, pp. 107-110).

According to Hofstee (2009, p. 108), a research method and a research design are often confused with one another. A research design, refers to the planned process that a researcher follows or plans to follow, in conducting a research study. While, a research method refers to the individual techniques used to accomplish a research objectives, such as the use of interviews to gather the data from individuals. It is reported that a research design typically conforms to one of two research paradigms, namely, qualitative research or quantitative research. The former, qualitative research, allows researchers to study social and cultural phenomena too, not relying solely on exact measurements, such as statistical values and calculations (Olivier, 2009, p. 111). While the latter, quantitative research, relies squarely on proving or disproving hypotheses through exact measurements of values obtained through experiments and mathematical calculations, among other methods (Myers, 1997).

Table 5.1, is a comparison of a few of the characteristics of the two research paradigms. Characteristics such as the origin of the paradigm, what it is typically used to measure, typical research methods used by research designs in that paradigm and the type of measurements of each paradigm are compared.

Research Paradigm	Qualitative	Quantitative
Origin	Social sciences	Natural sciences
Measures	A lot about few things	Little about a lot of things
Research Methods	Observation	Laboratory experiments
	Fieldwork	Econometrics
	Interviews	Mathematical modelling
	Questionnaires	Survey methods
Type	Social and cultural phenomena	Exact measurements

Table 5.1: A comparison of qualitative research versus quantitative research. Adapted from Olivier (2009, p. 111) and Myers (1997)

With regard to the selection of a research design to follow, Hancock and Algozzine (2011, p. 35) suggest that researchers should consider how well the selected research design will allow the full investigation of the research object. In other words, the researcher must consider the limitations presented by the research design, and the research paradigm, from which it originates. Due to SA SMMEs having many characteristics and constraints, which cannot be measured purely through quantitative methods, the research design followed by this research study leans towards the qualitative research paradigm.

Interestingly, it has been reported that the solutions of most scientific works lack practical relevance to the practitioners. This means that the practitioners are unable to implement those solutions in practice to exploit an opportunity or solve a 'real life' problem (Benbasat & Zmud, 1999). As the problem being investigated by this research study is a real-life problem, it was decided that a research design, which yields solutions of practical relevance would be most relevant to this study. Therefore, design-oriented IS research was selected, as the research design to be followed throughout this research study. Design-oriented IS research will be discussed in the next section of this chapter.

### 5.3 Design-oriented IS Research

Design-oriented IS research, yields solutions of practical relevance, while adhering to the four conditions of scientific works (showing scientific rigour), as discussed in section 5.2. Therefore, design-oriented IS research guides researchers in developing artefacts, such as constructs (examples include concepts, terminology and languages, models and frameworks, among others). The constructs developed through design-oriented IS research can even become solutions that are later developed, as prototypes or production systems (Österle et al., 2010). Thus, the artefacts developed by following a design-oriented IS research approach, are labelled as solving construction or inventive problems (Verschuren & Hartog, 2005).

Osterle et al. (2010), define four distinct phases that comprise the iterative process to be followed when conducting design-oriented IS research. Each phase of design-oriented IS research has a number of objectives, as can be seen below (numbered i-x):

1. The **Analysis Phase** is the phase in which the research study is initiated by the stakeholder (researcher, business practitioner, or others with a vested interest in the outcomes of the research study). Thus, a *practical business problem is identified* (i) and described, *research objectives, questions* (ii) and *gaps in the knowledge are specified* (iii). Furthermore, a *research plan* (iv) is put forward for the development and improvement of artefacts, using problem-solving methods that are known in either business or science, or in both. The fifth and final objective of the Analysis Phase, is for the researcher to *identify the external factors, which affect the research problem* (v).
2. The **Design Phase** is the second of the four phases of the design-oriented IS research approach. In this phase, the researcher should create the *proposed solution* (vi) through generally accepted methods. The researcher must then *justify the developed solution* (vii), or suggested improvements to existing artefacts, as much as possible. The proper justification of the developed

solution or improvements should include *contrasting this solution, with solutions already known in business and science* (viii).

3. Thirdly, the ***Evaluation Phase*** ensures that the proposed solution solves the identified research problem. In this phase, the proposed solution is *compared to the specified research objectives* (ix).
4. Finally, in the ***Diffusion Phase***, the findings of the research study are prepared for distribution to the target audience of the research study. Osterle et al., (2010), state that *research publications* (x), such as scientific papers, practitioner papers, conference papers, oral presentations and research dissertations are the best manner in which to distribute the findings of a design-oriented IS research study.

Thus, each of the objectives in design-oriented IS research can be mapped to the appropriate phase of design-oriented IS research. The mapping of the objectives of design-oriented IS research to the appropriate phase of design-oriented IS research is seen in Table 5.2, below.

<b>Phases of design-oriented IS re- search</b>	<b>Objectives</b>
<b>Analysis Phase</b>	(i) Identify a practical business problem (ii) Construct research objectives (iii) Identify gaps in knowledge (iv) Devise an appropriate research plan (v) Identify external factors
<b>Design Phase</b>	(vi) Create the proposed solution (vii) Justification of the proposed solution (viii) Compare proposed solution to existing solutions
<b>Evaluation Phase</b>	(ix) Evaluate proposed solution against research objectives
<b>Diffusion Phase</b>	(x) Research publications

Table 5.2: Design-oriented IS research objectives mapped to the appropriate research phase.

Figure 5.1, below, is a graphical representation of the four phased, iterative approach of design-oriented IS research, as defined by Osterle, et al., (2010). The consecutive phases of design-oriented IS research are shown through the use of arrows showing the direction of the research process. Design-oriented IS research forms a cyclical process, where the diffusion phase of a research study leads to the analysis phase of the next research study.

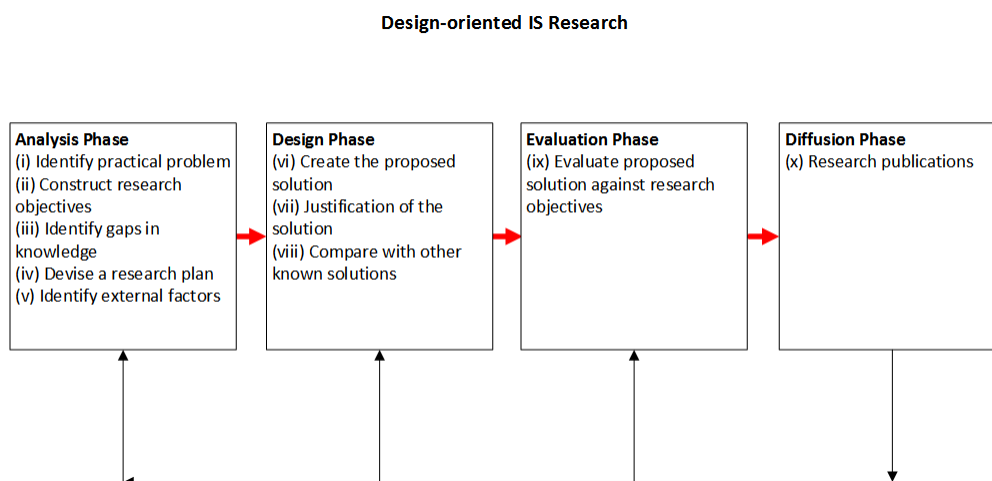


Figure 5.1: Design-oriented IS Research. Adapted from Osterle, et al. (2010)

Although design-oriented IS research studies often makes use of research methods taken from business, social sciences, computer engineering and sciences, researchers are still allowed their 'academic freedom'. This academic freedom allows researchers to decide on research objectives, research methods, the publication of research results and stakeholder satisfaction. However, a research study that claims to have followed the design-oriented IS research approach, must still adhere to four distinct research principles (Österle et al., 2010).

The four research principles of any design-oriented IS research study, as defined by Osterle et al. (2010) are:

- Firstly, ***abstraction***, which requires that each solution, artefact or improvement must be applicable to an entire class of problems, not just a single instance only;
- Secondly, ***originality***, meaning that an artefact, solution or improvement should make some form of contribution to furthering the body of knowledge;
- Thirdly, the ***justification*** of the developed artefact, solution or improvement and the conclusions reached must be clear. These justifications should allow for the validation of the findings of the research study; and



- Fourth and finally, is the *benefit* of artefact, solution or improvement developed by the research study. Each of these should yield a benefit for its stakeholders and intended targets, either immediately or in the future.

Furthermore, design-oriented IS research allows the researcher academic freedom that does not limit the researcher in fully investigating the research problem. Simply stated, design-oriented IS research allows the researcher to freely select research methods that would allow the researcher to best accomplish the research objectives of this research study (Österle et al., 2010). However, the academic freedom of design-oriented IS research can be seen as a limitation of the research design too. The research design offers researchers little guidance on the procedure to be followed in completing each of the phases of design-oriented IS research (Delport, 2017, p. 46). To overcome this limitation of design-oriented IS research, this research study combined design-oriented IS research with design-based research similar to that which Delport (2017, p. 46) suggests. Design-based research is discussed in the next section of this chapter.

## 5.4 Design-based Research

As mentioned in section 5.3, the identified limitation of design-oriented IS research was overcome by integrating this research design with design-based research. This section will discuss what design-based research is and its origin. Although both design-oriented IS research and design-based research share similar characteristics, such as to produce artefacts of scientific rigour and practical relevance, one of the differences between the two, is that design-based research stems from the learning sciences field of study (Barab & Squire, 2004).

Emerging in the twenty first century, design-based research was seen as the research design to bridge the gap between research and practice, in formal education (Anderson & Shattuck, 2012). Similarly, design-oriented IS research was intended to bridge the gap between academic works and practically implementable systems in the IS field (Österle & Otto, 2010). A further similarity of these two

research approaches, is that like design-oriented IS research, design-based research goes through a series of four iterative phases too (Anderson & Shattuck, 2012). The four phases of design-based research, as defined by Herrington, McKenney, Reeves and Oliver (2007), are seen below:

1. ***Phase 1: Analysis of practical problems by researchers and practitioners in collaboration.*** In this phase, three tasks are to be completed. The first task is to identify and explore a *research problem* (a). This task is crucial, as the problem statement will stem from the identification of a research problem. The solution to the research problem, will form the focus of the entire research study. Identifying a suitable research problem, should involve *the researcher and the practitioners* (b). However, it is reported that the involvement of practitioners might not be feasible in the initial phases of the research study. Thus, the role of practitioners can be seen through data collection at a later stage of the research study.

The second task of Phase 1, is the identification of appropriate research questions. Essentially, the research questions aim to present the researcher with attainable objectives in answering the research questions. Therefore, this research study defines *research objectives* (c), rather than research questions.

The third and final task of Phase 1, is to conduct a *literature review* (d) of previously published works in the field. A literature review in this phase, would seek to derive the draft principles to guide the design and the development of the solution.

2. ***Phase 2: The development of solutions informed by existing design principles and technological solutions.*** This phase again consists of three tasks that should be completed, before proceeding to Phase 3 of the research process. The first task to be completed is the construction of a *theoretical model* (e). It is reported that the theoretical model should be based on the literature, thereby forming the background theory of the research study. However, this theoretical model might have weak links to the theory, and be more related to the described research problem.

The theoretical model forms a basis for the proposed solution, as theory can then inform practical design guidelines (known as draft principles). The *draft principles* (f) are derived in the second task of Phase 2. As mentioned earlier, the draft principles guide the design and the development of the proposed solution. The draft principles will be largely based on the literature; but they can include other data collected from the practitioners. The *proposed solution can be described* (g), as the third task of Phase 2.

3. ***Phase 3: Iterative cycles of testing and the refinement of solutions in practice.*** This phase involves a number of iterations, which are determined by the outcome of the previous iteration. A typical research study would consist of at least one iteration, in which the proposed solution would be evaluated against the draft principles, which guided the design of the proposed solution. Pending the outcomes of the first iteration and its evaluation, a number of iterations may be necessary to ensure that the proposed solution adheres to the draft principles; and that it is suitable as a solution to the described research problem.

After each iteration, implementation and evaluation changes are made to the proposed solution to improve its ability to address the research problem. In each iteration, it is necessary to describe three specific elements. The first of these elements is the *participants* (h) of the iteration. It is reported that the participants for the evaluation of the proposed solution will depend on the

goal of the research study. Therefore, the participants are usually individuals affected by the research problem, or individuals who possess characteristics that warrant their expertise on the research problem.

The second element of an iteration involves a *data collection and analysis process* (i), in which the success of the proposed solution is evaluated. This is done by evaluating the proposed solution against the draft principles, as these are derived from the literature and other data related to addressing the research problem. Such data collection and analysis can involve either qualitative or quantitative data.

The third element of an iteration, is related to the *refinement and implementation* (j) of the proposed solution. Necessary changes to the proposed solution, as identified in the data collection and the data analysis, are made. Depending on the data collection and the data analysis findings, subsequent iterations might be necessary to re-evaluate the proposed solution after the necessary changes were made. Typically, the subsequent iterations will follow the same process as the first iteration and will have the same elements.

4. ***Phase 4: Reflection to produce design principles and to enhance the solution implementation.*** In Phase 4, the researcher is required to produce three forms of output from a research study.

The first of these outputs is *scientific outputs (design principles)* (k), which include evidence-based heuristics that can inform future development and implementation decisions. Such decisions may be a portrayal of the procedures, results and context, such that readers may determine which insights may be relevant to their own specific settings. Unlike draft principles (which guide the design of an artefact), design principles offer guidance on the context in which the artefact may be implemented and any prerequisites for creating better understanding in that context. Feedback and recommendations received during Phase 3, may also be considered as design principles;

where such feedback does not necessarily affect the developed artefact, but may have an effect on its implementation. Simply stated, design principles affect how the artefact is used; whereas, draft principles affect how the artefact is developed. An example of using draft principles would be establishing the characteristics of SMMEs and using the established characteristics to draft a solution appropriate (representative of the SMME characteristics) for SMMEs. While an example of design principles could include identifying the fundamental concepts that SMMEs would need to understand before being able to use the drafted solution.

Secondly, a researcher is required to produce *practical outputs (designed artefact)* (l), which could take the form of a software package. However, it is not necessary for the researcher to be the developer of such a software package. Software programmers or other interested parties can be the developers of such a software package, guided by the researcher.

The third form of output required from a researcher is a *societal output (professional development of participants)* (m). Through the collaboration of researchers and practitioners, all involved parties can benefit from professional development. This can include learning how to use the developed artefact to improve the productivity of an enterprise.

Table 5.3, below, summarises the discussions above. Each of the tasks to be completed of design-based research are mapped to their appropriate design-based research phase. Furthermore, the tasks to be completed are labelled alphabetically, according to the discussion above.

<b>Phases of Design-based Research</b>	<b>Tasks to be completed</b>
<b>Phase 1: Analysis of practical problems by researchers and practitioners in collaboration.</b>	(a) Statement of research problem (b) Consultation with researchers and practitioners (c) Research objectives (d) Literature review
<b>Phase 2: Development of solutions informed by existing design principles and technological innovations.</b>	(e) Theoretical model (f) Development of draft principles to guide design of the solution. (g) Description of the proposed solution Evaluation of the solution (Iterations)
<b>Phase 3: Iterative cycles of testing and refinement of solutions in practice.</b>	(h) Participants (i) Data collection and data analysis (j) Solution refinement and implementation
<b>Phase 4: Reflection to produce "design principles" and to enhance the solution implementation.</b>	(k) Design principles (l) Designed artefact (m) Professional development of participants

Table 5.3: Design-based Research mapped to typical research study elements. Adapted from Herrington, et al. (2007)

Figure 5.2, below, depicts the four phased iterative process of design-based research. As seen in the figure, the phases of design-based research, are similar to those of design-oriented IS research.

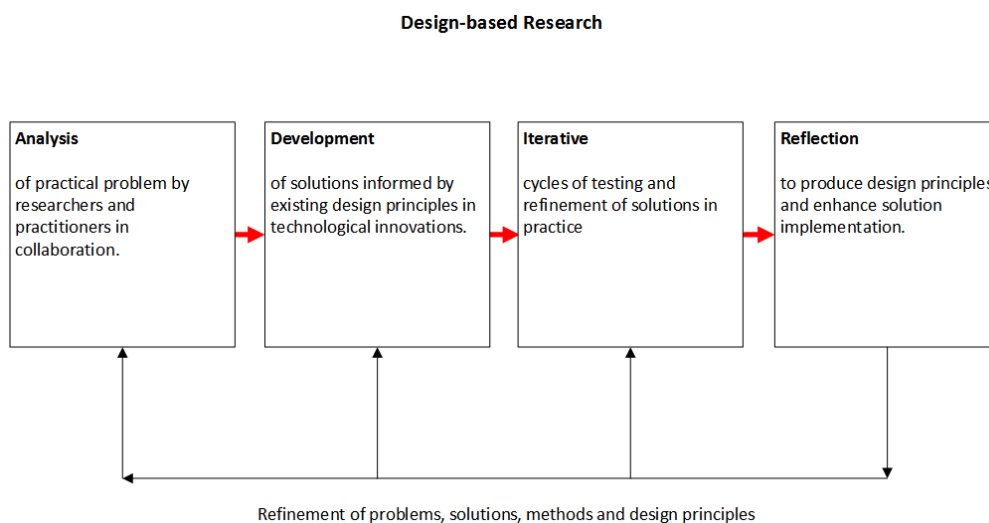


Figure 5.2: Design-based Research. Adapted from Herrington, et al. (2007)

This section of Chapter 5, has discussed the design-based research process. Furthermore, it was mentioned that design-based research and design-oriented IS research are similar; but they have some differences too. One of these differences being that design-based research provides explicit guidance for each of the tasks to be completed per phase of the research process. This difference can be used to overcome the limitation of design-oriented IS research, which is that design-oriented IS research provides little guidance on tasks for each phase of the research process.

Section 5.6, will discuss how design-oriented IS research and design-based research were integrated to formulate an integrated research design and how they were used in the context of this research study.

## 5.5 The Integrated Research Design

Sections 5.3 and 5.4 discussed design-oriented IS research and design-based research, respectively. Furthermore, in section 5.4, it was mentioned that the integration of design-oriented IS research and design-based research can assist in overcoming the mentioned limitations of design-oriented IS research. Therefore, this section will provide an account of how design-oriented IS research and design-based research were integrated. The integration of these two research designs will be discussed according to each of the four phases of the research designs. Tables were used to show how each objective of design-oriented IS research was mapped to the relevant task of design-based research. The Analysis Phase and Phase 1, are the first of the four phases to be discussed.

### The Analysis Phase and Phase 1

As seen in Table 5.2, the Analysis Phase of design-oriented IS research requires that the researcher completes objectives (i) to (iv). The first of the objectives is (i) *identifying a practical business problem*. Secondly, a researcher should (ii) *construct research objectives*. For the third objective, a researcher should (iii) *identify the gaps in knowledge*. Fourthly, (iv) *devising an appropriate plan to conduct the research study* is listed as the final objective for the design-oriented IS research Analysis Phase.

Similarly, as seen in Table 5.3, Phase 1 of design-based research, has four tasks that must be completed. Firstly, researchers must (a) *state a research problem*, which will form the focus of the research study. Secondly, researchers should (b) *consult other researchers and practitioners*; so that they too can play an active role in the investigation of the research problem.

The third task is about (c) *the establishment of appropriate research objectives related to the problem statement*. Finally, researchers are required to (d) *conduct a review of the literature related to the field of study to identify any gap in the knowledge*. Thus, where appropriate, each of tasks of Phase 1 of design-based



research were mapped to each of the objectives of the design-oriented IS research Analysis Phase.

Similarities, such as an objective and a task both referring to the identification of a research problem were used to map the objectives to tasks. It was concluded to be logical and useful to consult other researchers and to collaborate with practitioners (b), in order to gain insight into external factors, which affect the research problem (v). Therefore, although no obvious similarity is seen between objective (v) and task (b), the two were deemed as a necessary match. The objective of devising a research plan (iv) was the only objective for which an appropriate task of design-based research could not be identified. As this task is a requirement of submitting a research proposal (beyond the scope of this dissertation), this objective was omitted from the list of objectives and tasks considered in this dissertation.

Table 5.4 shows the mapping between the objectives of the Analysis Phase of design-oriented IS research and the tasks of Phase 1 of design-based research.

<b>Design-oriented IS Research Objectives</b>	<b>Design-based Research Tasks</b>
(i) Identify a practical business problem	(a) Statement of research problem
(ii) Construct research objectives	(c) Research objectives
(iii) Identify gaps in knowledge	(d) Literature review
(v) Identify external factors	(b) Consultation with researchers and practitioners

Table 5.4: Mapping design-oriented IS research Analysis Phase to design-based research Phase 1

## The Design Phase and Phase 2

This section is about the integration of the Design Phase of design-oriented IS research, with Phase 2 of the design-based research design. The Design Phase of design-oriented IS research consists of four objectives, as can be seen in Table 5.2.

The first of the three objectives is (vi), *to create the proposed solution to the*

*research problem*. In Table 5.3, the first task of design-based research (e) entails the *designing of a theoretical model*, which is based largely on the literature. Therefore, objective (vi) of design-oriented IS research can be seen as similar to task (e) of design-based research, warranting a match of the two.

The second objective of the Design Phase of design-oriented IS research, entails (vii) *justifying the proposed solution*. For the purposes of justifying the solution, the necessary aspects of the solution should be determined. These necessary aspects can be seen as the (f) *draft principles*, which are used by a researcher, to guide the design of the solution.

The third and final objective of the Design Phase design-oriented IS research (viii) entails *comparing the proposed solution with the existing solutions*. Thereby, through (g) *describing the proposed solution*, a researcher is able to compare and contrast the proposed solution with the existing solutions.

Thus, the complete mapping of design-oriented IS research Design Phase objectives, to design-based Phase 2 research tasks can be seen in Table 5.5.

<b>Design-oriented IS Research Objectives</b>	<b>Design-based Research Tasks</b>
(vi) Create the proposed solution	(e) Theoretical model
(vii) Justification of the solution	(f) Development of draft principles to guide design of the solution
(viii) Compare with other known solutions	(g) Description of the proposed solution

Table 5.5: Mapping design-oriented IS research Design Phase to design-based research Phase 2

### The Evaluation Phase and Phase 3

The Evaluation Phase of design-oriented IS research, has only one objective. In this objective, the researcher must (ix) *evaluate whether the proposed solution meets the research objectives of the study*. Further guidance on evaluating the proposed solution is obtainable from the tasks of Phase 3 of design-based research. In this

phase, the proposed solution is evaluated in a number of iterations, to ensure that it adheres to the draft principles derived in Phase 2.

The tasks of each iteration include (h) *selecting participants to evaluate the solution*; using appropriate research methods, such as interviews and focus groups to (i) *collect the data from the participants*. The data is then analysed and used to (j) *refine the solution*, which is implemented at the end of the iteration. These iterations continue until the findings of the data analysis indicate that the proposed solution is complete, according to the draft principles.

Table 5.6, is the Evaluation Phase that resulted from the integration of the Evaluation Phase of design-oriented IS research and Phase 3 of the design-based research.

Design-oriented IS Research Objectives	Design-based Research Tasks
(ix) Evaluate proposed solution against research objectives	<b>Evaluation of the solution</b>  (h) Participants (i) Data collection and data analysis (j) Solution refinement and implementation Further iterations of evaluation if necessary

Table 5.6: Mapping design-oriented IS research Evaluation Phase to design-based research Phase 3

### The Diffusion Phase and Phase 4

The Diffusion Phase of design-oriented research entails disseminating the findings of the research study. *Research publications* (x), such as scientific papers, dissertations and others, as mentioned in section 5.3, are suitable diffusion methods.

Phase 4 of design-based research, entails reflecting on the findings of the research study, to produce the design principles. The tasks to be completed in Phase

4 involve the production of (k) *design principles*, which would guide users in determining which aspects of the proposed solution best fit their setting. Additionally, the design principles could provide the researcher with the necessary insight; into creating the proper context for users to understand the artefact and its value.

Another task of this phase is, the (l) *designed artefact*, which may include software packages, must be published. Finally, there should be (m) *professional development of the participants*.

The professional development of the participants can include, but is not limited to, training on the use of the proposed solution.

Table 5.7 below, shows the mapping of the design-oriented Diffusion Phase objectives to the design-based research Phase 4 tasks.

<b>Design-oriented IS Research Objectives</b>	<b>Design-based Research Tasks</b>
(x) Research publications	(k) Design principles (l) Designed artefact (m) Professional development of participants

Table 5.7: Mapping design-oriented IS research Diffusion Phase to design-based research Phase 4

The above discussions gave an account of how design-oriented IS research was integrated with design-based research to form an integrated research design that was intended to overcome the limitations of design-oriented IS research, as discussed in section 5.4.

Furthermore, detail was given on how tasks from design-based research will be completed to address the objectives of design-oriented IS research. Thus, it can be concluded that the tasks of design-based research provide guidance on completing the objectives at each of the phases of the design-oriented IS research process.

The result of the integration is a four phased integrated research design, as described in the sections above. The integrated research design, adheres to the

four principles of design-oriented IS research, as discussed in section 5.3; while benefiting from the detailed guidance of design-based research.

The first of the four phases is named the *Analysis Phase*, according to the first phase of design-oriented IS research. In the Analysis Phase of the integrated research design, tasks (a) to (d), as seen in Table 5.4, are completed. The second phase of the integrated research design is named the *Design Phase*. The Design Phase entails completing tasks (e) to (g) of Table 5.5. Likewise, the third phase of the integrated research design is the *Evaluation Phase*. In the Evaluation Phase, the researcher must complete tasks (h) to (j) in iterations, as seen in Table 5.6. Fourth and finally, the research process ends in the *Diffusion Phase*. For the Diffusion Phase, tasks (k) to (m) must be completed, in order to disseminate the findings of the research study.

Table 5.8, summarises the above discussions of how each of the phases of design-oriented IS research and design-based research were integrated with each other.

Phase of Design-oriented IS Research	Phase of Design-based Research	Tasks to be completed
Analysis Phase	<b>Phase 1: Analysis of practical problems by researchers and practitioners in collaboration.</b>	(a) Statement of research problem (b) Consultation with researchers and practitioners (c) Research objectives (d) Literature review
Design Phase	<b>Phase 2: Development of solutions informed by existing design principles and technological innovations.</b>	(e) Theoretical model (f) Development of draft principles to guide design of the solution. (g) Description of the proposed solution.
Evaluation Phase	<b>Phase 3: Iterative cycles of testing and refinement of solutions in practice.</b>	<b>Evaluation of the solution (first iteration)</b>
		(h) Participants (i) Data collection and data analysis (j) Solution refinement and implementation <b>Evaluation of the solution (second and further iterations)</b>
		Participants Data collection Data analysis Solution refinement
Diffusion Phase	<b>Phase 4: Reflection to produce “design principles” and enhance solution implementation.</b>	(k) Design principles (l) Designed artefact (m) Professional development of participants

Table 5.8: A summary of the integration of the design-oriented IS research with the design-based research phases.

Figure 5.3, below, graphically represents the research process followed in the integrated research design. As seen in the figure, the research process followed in the integrated research design is similar to that of design-oriented IS research and design-based research as seen in Figure 5.1 and Figure 5.2, respectively.

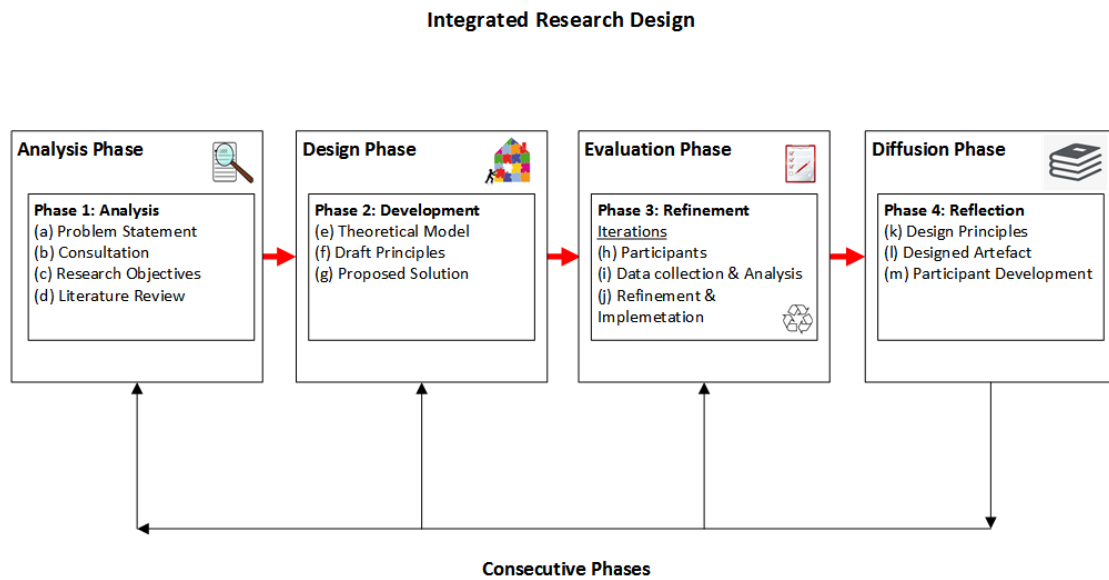


Figure 5.3: A diagram of the integrated research design. Adapted from Delpont (2017, p. 49)

The following section of this chapter will discuss how the tasks of each phase of the integrated research design were completed in the context of this research study.

## 5.6 Research Design in Context

In Section 5.5, the process of integrating the objectives of design-oriented research with the tasks of design-based research, was discussed. The discussion resulted in Table 5.8 and the research process Figure 5.3. This section will discuss how each of the phases of the integrated research design were completed in the context of conducting this research study.

The discussion will be structured, according to the flow of the process of the research design. Therefore, the first section was named the Analysis Phase, according to the first phase of the integrated research design. Throughout this section, numbers and labels will be used to match the tasks of the integrated research design (labelled alphabetically), to tasks completed in the process of this research study (labelled numerically).

An example of the above, can be seen by referring to Figure 5.4, where the labelled parts in this figure were completed by the researcher by performing the tasks, as numbered in Figure 5.6. A table is used at the end of the discussion of each phase, to show how each task (numbered part) of the research process, was matched to a task of the research design phase (labelled part). Due to space constraints within the table, only the labels and numbers are used in the table.

### 5.6.1 The Analysis Phase

The Analysis Phase, is the first phase of the integrated research design. As can be seen in Figure 5.4 below, the tasks for this phase are; (a) the problem statement, (b) consulting researchers and practitioners, (c) the research objectives, and (d) the literature review.



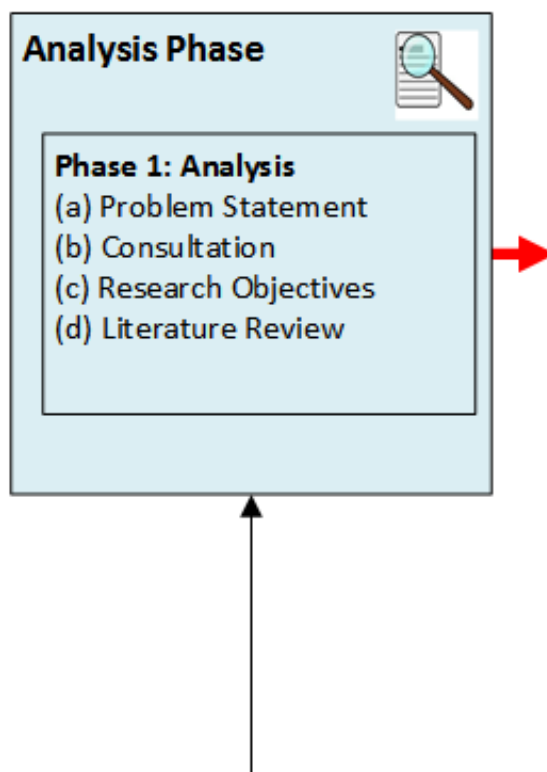


Figure 5.4: Analysis Phase of integrated research design

Thus, in completing the tasks of this phase, the researcher conducted a review of literature related to information security governance in SMMEs. The literature review was inspired by a review publication on the risk management practices of SA SMMEs, by Smit and Watkins (2012). In this review of SA SMME risk management practices, the authors discussed that many SMME owner-managers are ignorant of the information security risks that their organisations face. Furthermore, it is reported that many of these SMME owner-managers deploy information security risk management techniques in a reactive manner. This, along with other characteristics of SA SMMEs, such as those identified in Chapter 4 lead to the high failure rate of SMMEs. Thus, Smit and Watkins (Smit et al., 2012) suggested that it is necessary to embed a structured information security risk management approach within the organisation. More so, the structured information security risk management approach should be aligned with the vision (business and informa-

tion security objectives) of an organisation, while reducing the over-management of information security risks (Smit et al., 2012).

The researcher then turned to information security best practices and standards to identify such a structured information security risk management approach, as discussed above. The NIST SP 800-53 R4 (2013, p. 7), refers to a three-tiered risk management approach. This three-tiered risk management approach proposes that information security risk management is performed at Tier 1: Organisational Level, Tier 2: Mission/Business Processes Level and Tier 3: Information Systems Level. The relevant stakeholders of the organisation are present at each one of the three tiers. Thus, this information security risk management approach can be compared to the information security governance direct/control cycle, as discussed in section 2.2.2 of Chapter 2. Figure 5.5, below, shows the three-tiered information security risk management approach, as discussed above.

Furthermore, the NIST SP800-53 R4 (2013), calls for the categorisation of information assets, to determine the information security requirements of the organisation. Through the categorisation of its information assets, an organisation can determine the amount of information security required for each information asset; and ultimately, the appropriate information security controls to protect those information assets.

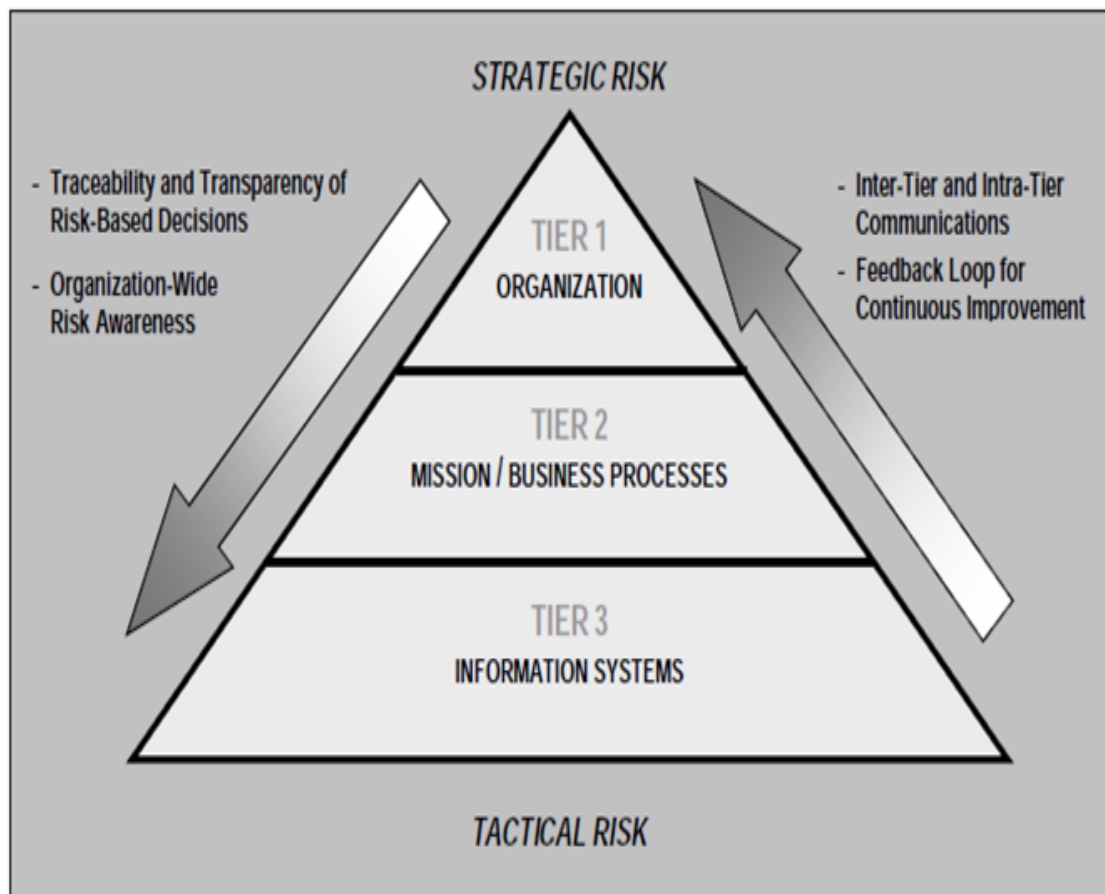


Figure 5.5: Three-tiered information security risk management approach. Adapted from NIST SP800-53 R4 (2013, p. 7)

Another well-known information security standard, ISO/IEC 27001 (2013), was also reviewed to identify a structured information security risk management approach, which could be embedded within the corporate governance structure of SA SMMs. In the ISO/IEC 27001 (2013, p. v) standard, organisations are given requirements for establishing, implementing, maintaining and continually improving an ISMS. ISO/IEC 27001 (2013, p. v), suggests that the development of an ISMS is influenced by four factors. The four factors, as listed in ISO/IEC (2013, p. v), are: the business and information security needs and objectives of an organisation, the information security requirements of an organisation, the

organisational processes used within the organisation and the size and structure of the organisation.

It was further discussed, in ISO/IEC 27002 (2013, p. vi), that it is essential for an organisation to determine its information security requirements, to avoid the over-management of information security risks. More so, the ISO/IEC 27003 (2010) , an ISMS implementation guide, requires that the information security requirements of an organisation should be determined prior to establishing an ISMS. The information security requirements become the input to the development process of the ISMS, as seen previously in Figure 2.6.4.

It therefore appeared that sufficient guidance existed for organisations to establish a structured information security risk management approach that can be embedded into the corporate governance of the organisation, and thereby prevent the over-management of information security risks. However, further discovery revealed that most of the well-known information security best practices and standards, are not inclusive of the unique characteristics and constraints of SMMEs, as discussed in Chapter 4. Additionally, the characteristics and constraints of SMMEs, make the use of most well-known information security best practices and standards too complex for SMMEs, as was discussed in section 4.9 of Chapter 4.

The discoveries as discussed above, led to the establishment of the problem statement of this research study, as seen in Chapter 1. The problem statement reads: (1) ***The unique characteristics of SMMEs make the current information security best practices and standards too complex for SA SMMEs to use in establishing the information security requirements aligned to the objectives of the enterprise..***

Therefore, it was hypothesised by means of thesis statement; that a model, simplified by being designed, according to the characteristics and constraints of SA SMMEs, would assist practitioners (SA SMME owner-managers) in solving the problem mentioned above. The researcher opted for the development of a model, as this type of artefact provides an exemplary structure of which certain of the

aspects applicable to the SMME can be used. Furthermore, a model acts as a blue print for future developments and the creation of a software package to automate the process (Tomhave, 2005, p. 8; Olivier, 2009, p. 45). The use and definition of the developed model, will be discussed further in Chapter 7.

In accordance with the hypothesis (thesis statement) of this research study, the primary objective of the research study became: (2) *to develop a simplified model to assist SA SMMEs in determining their information security requirements that are aligned with the unique characteristics and constraints of the organisation.* To establish how such a model should be developed, the researcher had to answer four questions, thereby completing four secondary research objectives.

Firstly, what is known about information security requirements? To answer this question, the researcher set out to obtain the perspective of various literature sources on the use and meaning of information security requirements. Secondly, what does an information security requirement comprise of? As information security best practices and standards are reported to provide expert knowledge; the researcher set out to establish from information security best practices and standards, what information security requirements comprise of (the criteria to classify an information security requirement). Thirdly, what characteristics would make an information security governance model simple enough to be used by SA SMMEs? To answer this question, the researcher had to establish the characteristics and constraints of SMMEs.

Furthermore, these characteristics and constraints affect the ability of an organisation, to implement a new system. Thus, the researcher had to determine the core elements that a model for SA SMMEs should possess. Fourth and finally, to ensure that the developed model is suitable to determine information security requirements, which lead to proper information security governance. Therefore, the researcher answered the question: What are the outcomes of good information security governance?

To answer each of the questions, as discussed above and accomplish each of the secondary research objectives, a (3) *literature review was conducted.* A literature

review, as defined by Olivier (2009, p. 8) entails identifying previous literary works relevant to the field of study, learning from these works and reporting on the findings. A formal definition of literature reviews will further be defined in section 5.7. Thus, the above discussions culminated in the Analysis Phase of this research study, taking the form as seen in Figure 5.4.

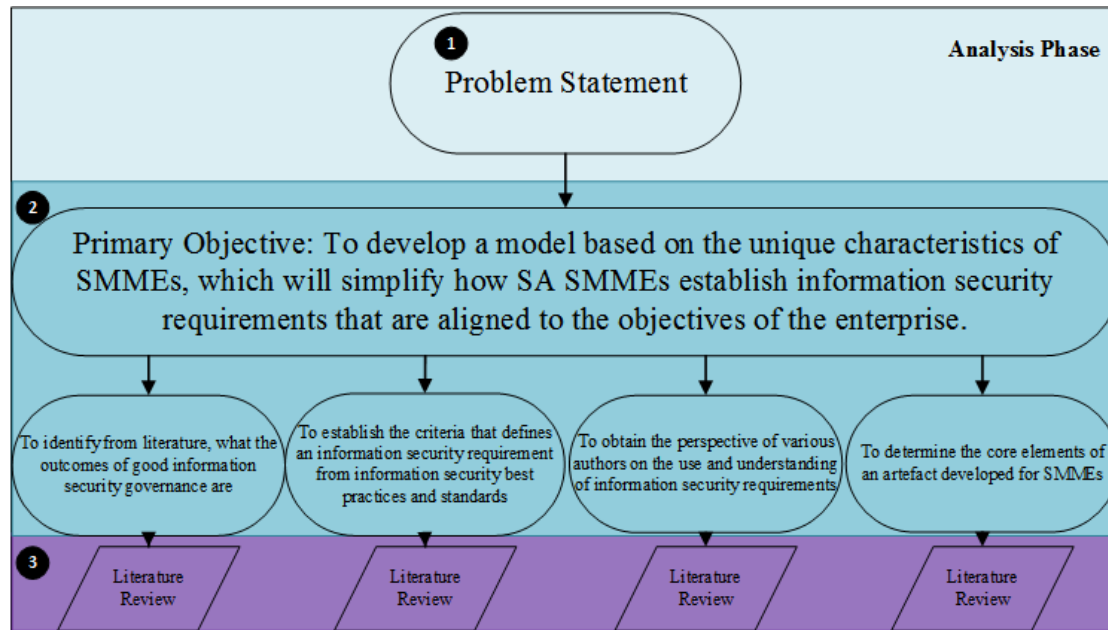


Figure 5.6: The Analysis Phase of integrated research design in the context of this research study

Table 5.9, shows how each of the numbered parts of the research process, as illustrated in Figure 5.6, were used to complete each of the tasks of the Analysis Phase of the integrated research design (labelled in Figure 5.4). Although, task (b) was not completed by the researcher, it was mentioned in section 5.4 that collaboration with practitioners is not always feasible in the Analysis Phase of the research study. However, collaboration with practitioners can still feature at a later stage within the research process (Herrington et al., 2007). Thus, in this research study, the researcher collaborates with SMME practitioners through the data collection in a survey, as discussed in Chapter 6.

Research Process	Integrated Research Design Task
1	a
2	c
3	d

Table 5.9: Mapping the tasks of the Analysis Phases of the integrated research design in the context of this study

This section has discussed how the researcher completed the tasks of the Analysis Phase of the integrated research study. It was discussed that a literature review was used to answer the questions and to partially address the secondary research objectives of this study. In section 5.6.2, the researcher will review the findings of the literature review.

### 5.6.2 The Design Phase

The second phase of the integrated research design is known as the Design Phase. According to this phase, researchers are required to complete three tasks. Firstly, a (d) theoretical model based on the literature must be constructed. Secondly, (e) the draft principles must be derived, to guide the design of the proposed solution. Thirdly, the researcher should provide a description of the proposed solution (f). Thus, the Design Phase of the integrated research design is as seen in Figure 5.7, below. This section of the chapter will discuss how the tasks of the Design Phase of the integrated research design were completed in the context of this research study.

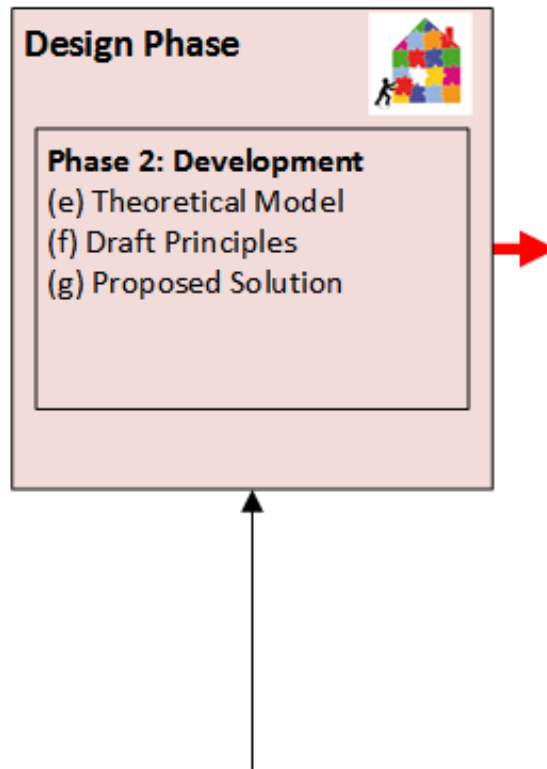


Figure 5.7: Design Phase of integrated research design

In addressing the first task of the Design Phase, the findings of the literature review were used to construct a theoretical model (4). The theoretical model was based on three findings from the literature review. The findings mentioned above are as follows:

- i Firstly, the criteria for determining an information security requirement were determined by reviewing the information security best practices and standards (see Chapter 3).
- ii Secondly, the use of checklists and guidelines to assist organisations in determining their information security requirements, were also discovered from the literature (see Chapter 3).
- iii Thirdly, the process and outcomes of good information security governance



(see Chapter 2) were used to structure a model based on the literature (theoretical model).

In particular, the theoretical model was structured, based on the direct/control cycle by von Solms and von Solms (2008), Figure 2.2.2 in Chapter 2. However, the direct/control cycle is based on a three-tiered corporate governance structure, common to large organisations. Thus, it was concluded that the theoretical model was not inclusive of the unique characteristics and constraints of SMMEs. The unique characteristics and constraints of SMMEs determined the fundamental components of the model (core elements).

Therefore, the researcher had to determine the core elements that would make a model suitable for SMMEs. In doing so, the researcher reviewed the literature to identify the characteristics and constraints of SMMEs, challenges to the success of SMMEs, and the challenges related to the implementation of information security best practices and standards in SMMEs (input for constructing the model). Among the characteristics of SMMEs, it was determined that SMMEs are rapidly evolving; and they generally have an owner-manager or CEO-centric corporate governance structure. Furthermore, the constraints and challenges of SMMEs, such as a lack of finance and limited expertise, are challenges to the implementation of information security best practices and standards in SMMEs.

A review of the literature, such as that of Hutchinson, Armit and Edwards-Lear (Hutchinson et al., 2014) and van Niekerk and Labuschagne (Van Niekerk & Labuschagne, 2006) led to a discovery about the use of information security best practices and standards in SMMEs. It was discovered that most well-known information security best practices and standards are resource intensive; and that they are built to fit corporate governance structures that are uncommon to most SMMEs. Thus, it was evident that the characteristics and constraints, along with the other discoveries about SMMEs, as seen in Chapter 4, should form the core elements of a model developed for SMMEs. Therefore, six core elements were identified from the literature review as seen in section 4.10 of Chapter 4. The six

core elements are scalability, simplicity, feasibility, utility, transparency and risk control.

Having identified all input, as discussed above (criteria, perspective, outcomes of good IS governance and core elements), a survey was conducted. The survey took the form of a questionnaire, which, in accordance with Olivier (2009, p. 78), is a structured set of questions to gather the characteristics of a population to show an association between these characteristics. Thus, the survey findings showed an association between the characteristics and the constraints of SMMEs and the complexity of implementing information security best practices and standards in SMMEs. However, as discussed in section 6.6 of Chapter 6, the survey conducted in this research study was intended only to describe a phenomenon about the participating SMMEs, and not to produce results reflective of the general population of SA SMMEs (not statistical). Therefore, descriptive statistics as defined by Huysamen (1998), were used to summarise the data obtained through the use of graphs and frequency tables, as can be seen in Chapter 6.

Overall, the purpose of the survey was to triangulate the findings of the literature review, to confirm that the claims of authors regarding SMMEs are true in the SA context also. According to Myers (1997), in triangulation knowledge which has already been discovered, is re-evaluated in a different context; in an attempt to determine whether the characteristics also hold true for that scenario. In section 5.6.1, it was mentioned that the researcher and the practitioner collaboration as required by the research design; was not done initially. However, it was reported that this collaboration would occur in a later phase of the research study. The survey allowed for the researcher and practitioner collaboration, which was reported to occur at a later phase of the research study.

Thus, by determining that the findings of the literature review and the core elements hold true for the SA SMME context (through the survey in Chapter 6), the researcher was able via a process of argumentation, to derive the draft principles (see section 7.2 of Chapter 7). The purpose of the survey was to confirm that the core elements and findings from literature were true in the SA SMME

context (triangulation), before the draft principles could be derived in Chapter 7. The draft principles were used to guide the design and development of the model developed, as the proposed solution to the research problem to be solved by this research study. Due to the influence of the discoveries from the literature and the findings of the survey, on the derived (5) draft principles, it may be said that the researcher argued evidentially. According to Mason (2002, p. 176), arguing evidentially involves presenting evidence to support a conclusion. Similarly, in this research study, the researcher used the discovery and the findings about SMMEs, information security requirements and the use of information security best practices and standards in SMMEs; to provide evidence of the need for a simplified model to be used by SA SMMEs; and the draft principles that this model should adhere to, in order for it to be suitable to be used by SA SMMEs. Thus, the draft principles, as discussed in Chapter 7, were used to guide the modelling process through which the model was designed and developed.

Therefore, the (6) *draft of the model developed*, as the proposed solution to the research problem of this study, became the output of the Design Phase. The draft model described the model proposed, as a solution to the research problem. A proof of concept prototype, (7) *automated tool* was then developed, based on the draft model. The prototype was an Excel spreadsheet, which automated the processes of the developed draft model. Thus, demonstrating the feasibility and the practicality of the model as SMMEs could use the automated tool to establish their information security requirements. Although automated, the tool still requires that users input data relating their enterprise. The tool then automatically generates an information security directive containing the information security requirements of the enterprise.

As seen in Figure 5.8, each of the numbered parts discussed above combined to form part of the Design Phase of the integrated research design.

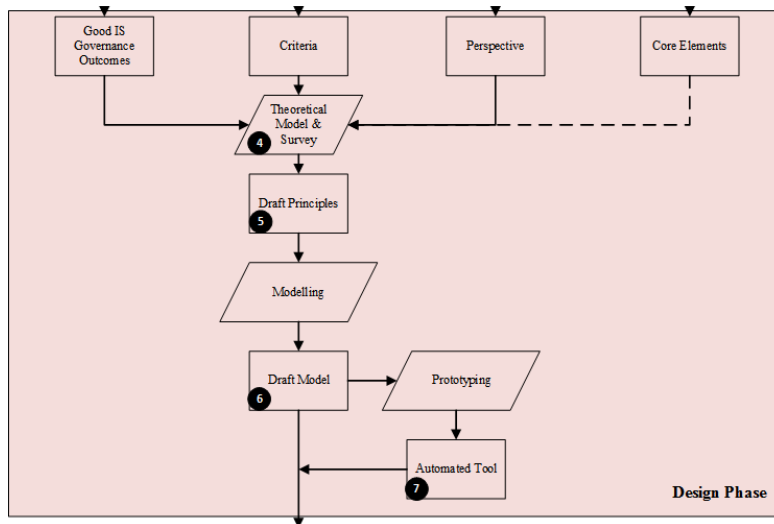


Figure 5.8: Design Phase of Design-oriented IS Research in the context of this research study

Each of the numbered parts of Figure 5.8, addressed particular tasks of the Design Phase of the integrated research design (as labelled in Figure 5.7), seen in Table 5.10 , below.

Research Process	Integrated Research Design Task
4	e
5	f
6 & 7	g

Table 5.10: Mapping the tasks of Design Phase of the integrated research design in the context of this study

This section has discussed the Design Phase of the integrated research design, in the context that was used in this research study. Each of the tasks to be completed in this phase had a specific outcome, which became an input to the draft principles, which were derived to guide the design and development of the model proposed, as the solution to the research problem identified in Chapter 1. Thus, a first draft of the model, became the output of the Design Phase of the

integrated research design. In the Evaluation Phase of the integrated research design, the first draft of the model will be evaluated and refined according, to the data collected from the practitioners.

### 5.6.3 The Evaluation Phase

It was mentioned at the end of section 5.6.2 that it is necessary for the proposed model to undergo iterative processes of evaluation. After each iteration of evaluation, the necessary refinement of the model must be made. The researcher should then make another attempt at implementing the model. This iterative evaluation process is in-line with both the Evaluation Phase of design-oriented IS research (Österle et al., 2010) and Phase 3 of design-based research (Herrington et al., 2007).

Therefore, this section of the chapter will briefly define the research methods used to collaborate with the practitioners and to collect the necessary data for the evaluation of the proposed solution. However, the manner in which each research method was used in the context of this research study, will be discussed in section 5.7.

The tasks to be completed in the Evaluation Phase of the integrated research design, are: (h) identifying the practitioners as participants for the evaluation process. Secondly, the researcher is required to: (i) collect the data related to the perception and the opinion of practitioners pertaining to the proposed model. The third task involves: (j) making the necessary refinements to the solution, as established through the analysis of the data collected from the practitioners. These tasks are as can be seen in Figure 5.9.

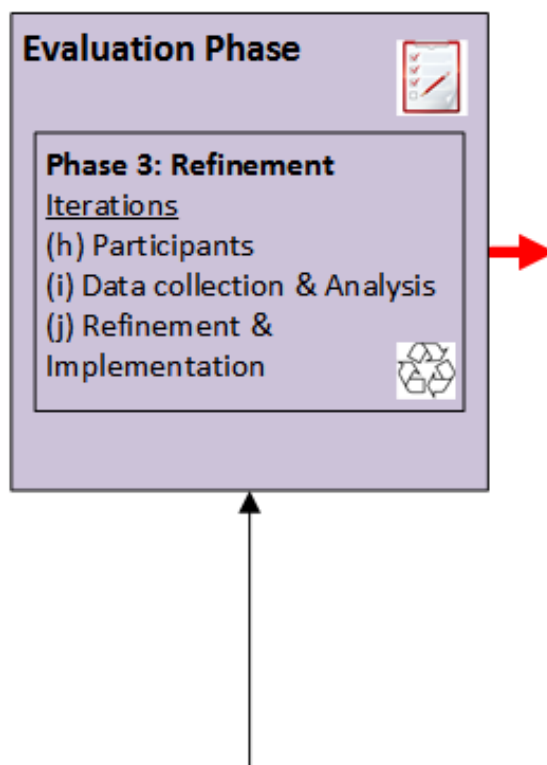


Figure 5.9: Design Phase of integrated research design

As seen in Figure 5.7 and discussed above the first task in the iterative process of the Evaluation Phase of the integrated research design is to identify the participants for the evaluation of the proposed model; and also the selection of the participants for the evaluation of the proposed solution is dependent on the research method used to gather the data from the participants.

Therefore, in an expert interview, participants who are considered to be experts, due to their knowledge and/or experience in a specific research area are selected, as the correct participants to interview. Furthermore the knowledge accessed by the researcher when interviewing these individuals, as participants of the expert interview (8), might otherwise not be accessible to the researcher from another source. However, access to experts is often a challenge; as these individuals keep to a tight schedule (Bogner, Beate, & Menz, 2009, p. 98). Thus, only one interview was held with the experts consulted in this research study. Furthermore,

it is reported that experts possess both practical and theoretical or interpretative knowledge, making the input of data collected from these individuals, highly valuable to the research study (Bogner et al., 2009, p. 100).

For the evaluation of the artefact developed through this research study, two expert interviews were conducted. One of the expert interviews was conducted to evaluate the developed model; while a second expert interview was conducted to evaluate the automated tool. To verify the model that was developed, an individual deemed as an information security expert for the purposes of this study, was interviewed. The information security expert was furnished with a suite of background information about the the research study. In addition to this background information, the draft principles which guided the development of the model were also presented to the information security expert.

The information security expert was then presented with a set of questions designed to evaluate whether the proposed model complies with the draft principles. Additionally, the questionnaire used for the information security interview expert contained questions about the model adhering to the outcomes of good information security governance.

In addition to the model that was developed as the solution to the research problem of this research study, an automated tool was developed based on the model. The automated tool was developed as proof of the concept, to demonstrate that the proposed model can be used to develop systems simple enough to be used by SA SMMEs, while adhering to the draft principles used to design and develop the proposed model. Thus, according to Olivier (2009, p. 51), the automated tool is known as a proof-of-concept prototype. Proof-of-concept prototypes are simplified programs or systems that simply seek to demonstrate the practicality of the model.

Another expert interview was conducted to evaluate the automated tool. For the purposes of evaluating the automated tool, an individual considered as a SA SMME expert was interviewed. The automated tool was also evaluated for adherence to the draft principles that were used to guide the design and the development

of the proposed model. Similar to the information security expert interview; the SMME expert was also furnished with the background information about the research study and the draft principles. Questions were then asked, to obtain the opinion of the SMME expert on the suitability of the automated tool for use in SA SMMEs.

Both experts interviewed were parties external to the research institution of the researcher. Due to geographical constraints and differences in time zones, both of the expert interviews were conducted by means of a questionnaire, which was sent via electronic mail, as explained in Chapter 8. As the draft principles were based on information security in SMMEs, the information security expert was deemed fit to perform the evaluation.

Furthermore, the questionnaire that was used to evaluate the automated tool; was designed to avoid the use of technical jargon, to avoid confusing the SMME expert. The data collected from both expert interviews were analysed; and revisions were made to the relevant artefact or noted for inclusion as design principles.

The resulting version of the model and the automated tool were then considered and recorded as the final version for this study. The procedure followed for conducting the expert interviews, the selection of the experts and the collection and analysis of the data, as well as the refinement of the artefacts will feature in Chapter 8. Details pertaining to the definition of an expert interview will be further discussed in section 5.7.

Thus, from the discussions above, it may be reported that the final model was evaluated by an information security expert through the researcher conducting an expert interview. Further, the automated tool was evaluated by a SA SMME expert, also by means of an expert interview.

Hence, the information security expert and the SMME expert were the (h) participants of the expert interviews. Following an explanation of the research problem, the background and the draft principles, the (i) data was collected from the experts by means of a questionnaire and analysed to identify any necessary



amendments to the proposed model and the automated tool. Based on the identified necessary amendments, the proposed model was (j) refined; and a final model was constructed. Recommendations from the SMME expert interview were beyond the scope of this study and were instead recorded as design principles. Further, recommendations from the information security expert interview were also considered as input to the design principles. As stated earlier in this chapter, design principles provide guidance on the implementation of an artefact developed through design-based research.

Based on the discussion of this section, the process followed in this research study, in completing the Evaluation Phase of the integrated research design is as seen in Figure 5.10 below.



Figure 5.10: Evaluation Phase of Design-oriented IS Research in the context of this research study

It can thus be concluded that number 8 of Figure 5.10 addressed the tasks that were completed for the Evaluation Phase of the integrated research design, in the context of this research study. Table 5.11, below, shows how each of these tasks is represented by the numbered activity from the research process, as can be seen in Figure 5.10.

Research Process	Integrated Research Design Task
8	h, i & j

Table 5.11: Mapping the tasks of the Evaluation Phase of the integrated research design in the context of this study

The following section of this chapter will discuss how the final of the four phases of the integrated research design was completed in the context of this research study.

#### **5.6.4 The Diffusion Phase**

As with the three previous sections, this section will discuss how a phase of the integrated research design, was completed in the context of this research study. The phase to be discussed in this section, is the fourth and final phase of the integrated research design; and this is known as the Diffusion Phase. The Diffusion Phase is also the fourth phase of design-oriented IS research. According to Osterle and others (2010), the Diffusion Phase entails distributing the findings of the research study to the appropriate audience.

Design-based research, Phase 4, suggests that the dissemination of the findings of the research study should be done by publishing (k) the design principles to guide the implementation of the solution, (l) the designed artefact and by professionally developing the participants (m) of the research study (Herrington et al., 2007). Thus, the completion of these three tasks became the objective of the Diffusion Phase of the integrated research design, as seen in Figure 5.11, below.

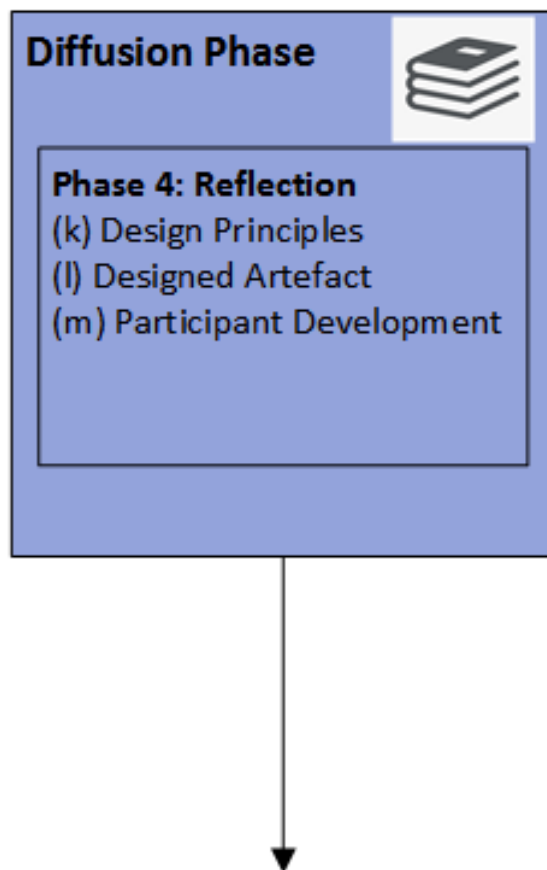


Figure 5.11: Design Phase of integrated research design

The design principles, include instruction manuals and training, which offer procedural guidance on the implementation and the future development of the solution. Unlike draft principles, which guide the design and development of the solution, design principles influence the manner in which the solution is implemented by the users. Thus, through the interview of the SMME expert (see section 5.6.3), the researcher was able to obtain further insight into the implementation of the model in SA SMMEs.

Insight was obtained by collecting and analysing the data related to the use, by the SMME expert. Furthermore, the (k) model itself fulfils the role of guidance on the implementation and future development of the automated tool. Each pro-

cess of the model is suggested as optional or mandatory, based on the category of SMME (micro, small or medium). Where, the smallest of the categories of enterprise, implements the least number of mandatory processes. Thus, the conditions for determining which aspects of the model apply to the category of SMME, can be determined through the first process of the model. The designed artefact (l), presented in this phase of the study included both the model and the resultant automated tool. Through research publications, such as scientific papers and conference presentations, the findings of this research study can be shared with the greater research community (m). Using the recommendations from the previous phase (Evaluation), the final versions of both the model and the automated tool (9) were developed as can be seen in Chapter 8.

Thus, the integrated research design Diffusion Phase, formed part of the research process of this research study, as can be seen in Figure 5.12 below.



Figure 5.12: Diffusion Phase of Design-oriented IS Research in the context of this research study

The labelled elements of the research process in Figure 5.12, addressed each of the numbered tasks of the Diffusion Phase of the integrated research design, as seen in Table 5.7.

Research Process	Integrated Research Design Task
9	k,l & m

Table 5.12: Mapping the tasks of Diffusion Phase of the integrated research design in the context of this study

Section 5.6 discussed how each of the four phases of the integrated research design were conducted in the context of this research study. More so, the reader

was shown how each of the tasks were addressed by an element of the research process. The following section of this chapter will attempt to elaborate on the definition and context of the use of each of the research methods implement in this research study.

## 5.7 The Research Methods

As mentioned in section 5.2, the research methods in the context of this research study, refer to the individual techniques used to accomplish a specific research objective, such as a literature review or modelling techniques (Hofstee, 2009, p. 108). Furthermore, pertaining to research methods and the research design used in this research study; it was mentioned that design-oriented IS research presents the researcher academic freedom to select the appropriate research methods to accomplish the research objectives of their research study (Österle et al., 2010).

Similarly, design-based research, which formed part of the integrated research design too, is not prescriptive of research methods to be used in completing the research process (Herrington et al., 2007). However, a commonality between the two research designs (design-based research and design-oriented IS research), is the indication of the need to establish a background in previously published literature, to properly define the research problem (Österle et al., 2010; Herrington et al., 2007). Therefore, as discussed in section 5.6.1 of this chapter, as literature review was conducted to establish a background of the problem area of this research study. This section will discuss how each of the research methods mentioned in section 5.6 were used in the context of this research study. The section will discuss the research methods, as they were used in each phase of the integrated research design.

### 5.7.1 The Analysis Phase: A Literature Review

Confucius once wrote *“a man who reviews the old, so as to find out the new, is qualified to teach others”*. Thus, it is common for a research study to begin by

reviewing the relevant literature in the area of research, published by other authors prior to the researcher embarking on the current research study.

Therefore, in academic or scholarly works, a literature review is often referred to as an anchor for a thesis or dissertation. According to Fink (2005, p. 3) and Okoli and Schabram (2010), a literature review is a research method that consists of three parts. Firstly, identifying relevant work from the complete and recorded body of knowledge. Secondly, evaluating the identified work to answer practical questions. Thirdly, the answers to the questions are used to draw conclusions on the existing research in that field. Thus, the literature review conducted in the Analysis Phase of the integrated research design used in this research study, was done, according to the definition above.

It is of importance to consider that the initial enquiry of this research study was influenced by a literature publication of risk management in SA SMMEs, by Smit and Watkins (2012). The discovery that most SA SMMEs were implementing ad hoc information security controls, while others were over-managing information security risk, prompted the need to determine the existence of an efficient information security risk management approach to avoid the phenomenon described above. Importantly, such an efficient information security risk management approach would have to form part of the overall corporate governance of the organisation (meaning SMME, as mentioned in an earlier chapter). Thus, it became evident that such an information security approach, would be an information security governance approach, rather than an information security risk management approach.

The process of information security governance was discussed in Chapter 2. Thus, a literature review on information security governance approaches and information security risk management approaches was conducted. The results of the literature review, eluded to the conclusion that an organisation should develop, implement and maintain an information security management system (ISMS). Thus, the literature review continued on the path of developing, implementing and maintaining an ISMS.

The results of the literature review on ISMS development and maintenance, resulted in four discoveries. Firstly, ISO/IEC27001 (2013, p. v), a well-known information security best practice and standard, calls for the development of an ISMS and the selection of information security controls from ISO/IEC27002. ISO/IEC27002 (2013, p. v), calls for the establishment of information security requirements, so that an organisation can determine the level of information security that it needs.

Furthermore, in ISO/IEC27003 (2010), organisations are required to perform an information security requirements analysis to determine the information security requirements of the organisation, which will be used as input in developing the ISMS. Related literature, criticised the sole use of an information security risk assessment to determine the information security controls to be used to protect the information assets of the organisation, as discussed in Chapter 3. However, substantial evidence was discovered from the literature, suggesting that most information security best practices and standards are too complex for the use of most SMMEs, resulting in the problem statement of this research study (see Chapter 1).

To understanding the problem better, in order to propose a solution, the author resolved to learn from the literature, including information security best practices and standards, to address the secondary objectives of the research study. As information security requirements had been defined in information security best practices and standards, the researcher resolved to using this criterion to define an information security requirement. Furthermore, information security best practices and standards are reported to be written based, on the knowledge of information security experts, as discussed in Chapter 2.

Secondly, as the over-management of information security was discovered through the literature, the perspective of authors on the use of information security requirements, in order to better understand the information security needs of an organisation were considered. Thirdly, as the information security approach should ultimately have contributed to information security governance within the organ-

isation, it was necessary to ensure that the proposed solution would contribute to the proper governance of information security. Thus, the outcomes of good information security governance were determined through the literature review.

Finally, to make the proposed solution more suitable to the SMME environment, the core elements of any artefact that is developed for SMMEs were also determined through the literature review. The use of a literature review to complete the four secondary research objectives, as mentioned above, concluded with the research methods used in the Analysis Phase of the integrated research design.

The following section, will discuss the research methods used in the Design Phase of the integrated research design.

### **5.7.2 The Design Phase: A Survey, Argumentation, Modelling, Prototyping and Triangulation**

As seen in section 5.6.2, the Design Phase of this research study, various research methods were used to derive the draft principles and to develop the proposed solution. The various research methods used, included surveys, argumentation, modelling, prototyping and triangulation. This section of the chapter will define the context in which these research methods were used for this research study.

Gable (1994) defined a survey as a group of data collection methods. One of the most common survey tools is a questionnaire, which is defined as a standardised set of questions to collect the data from a group that is representative of a large population. The representative group is known as the sample population. In a statistical study, the findings from the data collected and analysed from the sample population, are generalised to a larger population, with the same characteristics as the sample population (Olivier, 2009, p. 81; Rattray & Jones, 2007). However, this was not a statistical study the data was not collected from a sample population large enough to be representative of the larger population of SMMEs in SA.

The purpose of the survey was to confirm that the findings from the literature were indeed applicable to the SMME sector in SA. Therefore, a questionnaire was



designed, with the criteria, perspective and good information security governance outcomes, as the input. However, despite numerous efforts, a sample population large enough to represent the data generalisable to the SMME sector in SA was not obtained. For this reason, descriptive statistics were used to describe the findings of the survey, instead of a statistical analysis. Huysamen (1998), claimed that descriptive statistics is concerned with drawing conclusions from the data by means of summarisation or description, where the sample from which the data was collected, is too small to form a representative sample of the general population. Therefore, the collected data is described by using percentages, frequency tables and graphs.

Additionally, the review of previously published literature in the Analysis Phase of the research study established the problem area of this research study. The use of a survey to confirm the established problem in SA SMMEs, is known as triangulation. It was reported earlier (section 5.6.2) that triangulation is the process of re-evaluating discovered knowledge in a different context (Myers, 1997). Thus, in accordance with Myers (1997), triangulation was performed by, re-evaluating findings on SMMEs from previously published literature, in the SA SMME context by means of a survey.

As defined by Mason (2002, p. 176), evidential argumentation entails presenting evidence in a logical manner to support a conclusion or a decision. Thus, the presentation of evidence in the form of existing knowledge collected through the literature review and the survey, can be defined as evidential argumentation. The results of the evidential argumentation in this research study are the draft principles (discussed in Chapter 7). These draft principles were used in guiding the modelling process, which entails constructing a graphical representation of new systems, to design and develop the proposed model (the first draft of the model).

Olivier (2009, p. 45), describes modelling as the process of constructing a graphical representation, which could form the blue-print of the new systems. The modelling process was used in constructing the proposed solution to the research problem that was identified in this research study.

In addition to the model developed as the proposed solution to this research study, the researcher developed an automated tool. The automated tool was developed to demonstrate the practicality and feasibility of using the processes of the model. Therefore, the automated tool was developed, based on the proposed model. Thus, in accordance with the definition discussed in an earlier section, the automated tool was developed as a proof-of-concept prototype. The proof-of-concept prototype is used to demonstrate that the idea has merit; and that it is of practical relevance. In simpler terms, a proof-of-concept prototype proves that the proposed blue-print (the model), can be developed into a practically implementable tool (Olivier, 2009).

The collection and analysis of the data in the survey process will be discussed further in Chapter 6. While the construction of the proposed model will feature in Chapter 7. The next section of this chapter, will discuss how two expert interviews were used to evaluate the proposed model and the automated tool, respectively, in the Evaluation Phase.

### **5.7.3 The Evaluation Phase: Expert Interviews**

The design-based research Phase 3 defines the need to have iterative cycles of evaluation for the refinement of the proposed solution (Herrington et al., 2007). Thus, this section will define the context in which the expert interviews were used to evaluate the proposed solution to the research problem of this study.

Littig (2009, p. 98), defined an expert interview, as interviewing individuals considered as experts in their field of research. These individuals are considered as experts, due to their vast knowledge and experience in a particular research field. However, it is also reported that expert interviews are often confused with elite reviews. Elite interviews are interviews conducted with individuals who have vast knowledge in a research field. Furthermore, elite individuals have a considerable sense of influence nationally and internationally, on the decisions made in their field of profession. Therefore, an expert can be elite; however, it is not always the case that an expert is elite.

This research study was only concerned with the knowledge and experience of the individuals; therefore, the elite status of the individuals was not considered. Due to their vast knowledge and experience, the experts were able to offer recommendations on the suitability of the proposed solutions for both the use of SA SMMEs and to the governance of information security.

The above discussion concludes the defining of research methods used in the research process throughout this research study. The next section of this chapter briefly revisits the key concepts presented in this chapter, to ensure that the objectives of the chapter have been met.

## 5.8 Conclusion

The objective of this chapter was to discuss the systematic approach that was used throughout this research study. Therefore, the design-oriented IS research and design-based research were defined. The author then discussed how these two research approaches were combined to form an integrated research design used throughout this research study.

Moreover, the use of the unique integrated research design was presented to the reader, according to the output of each phase. Therefore, the research methods used to accomplish the research objectives of this study were also discussed. Thus, it may be concluded that the objective of this chapter has been met. Further details pertaining to the evaluation of the developed model and automated tool can be found in Chapter 8.

The next chapter will discuss the process followed in developing the questionnaire, which was the survey data collection tool used for this research study, as mentioned in section 5.6.1 of this chapter.

# Chapter 6

## A Survey of SA SMMEs

*“The fact that an opinion has been widely held is no evidence whatever that it is not utterly absurd.” -Bertrand Russell*

### 6.1 Introduction

The integrated research design used throughout this research study, requires researcher and practitioner collaboration, as discussed in section 5.6.1 of Chapter 5. For the purposes of this research study, the researcher and the practitioner collaboration was in the form of a survey, which was conducted by means of a questionnaire. Furthermore, Olivier (2009, p. 51) reports that a researcher is often required to support the identified research problem by providing evidence from primary sources. Primary sources are defined as the object of investigation, which refers to SA SMMEs in the context of this research study.

The objective of this chapter is, therefore, *to define the method followed in developing the questionnaire used to collect the data from SA SMME practitioners and to discuss the findings concluded from the collected data.*

This chapter is structured, according to the seven step survey conducting method, as defined by Olivier (2009, p. 79). Thus, the reader can expect to be

informed about the tasks completed by the researcher in each of the seven steps.

Firstly, the researcher will establish a theory to validate through the survey. Secondly, the researcher is required to formulate a hypothesis about the theory. The third step involves the definition and selection of the population sample to be studied. For the fourth step, the researcher must distribute the questionnaire to collect the data from the sample population. The analysis of the collected data is done in the fifth step of the method. Typically, the data analysis step involves making statistical inferences about the general population from the collected data. However, this research study is of the qualitative paradigm and not the quantitative paradigm. Furthermore, the received responses from the sample population of the survey were too low to make any statistical inferences about the general population. Therefore, no statistical inferences were made from the data collected through this survey. Thus, the researcher will discuss how descriptive statistics were used, as an alternative to statistical inference.

In the sixth step, after analysing the results, the researcher evaluates whether or not the hypothesis formulated in step two is correct. The correctness of the hypothesis has a direct bearing on the validity of the theory established in the first step. Therefore, the researcher determines the validity of the theory based on the correctness of the hypothesis, in step seven.

Finally, in the concluding section of this chapter, the researcher reviews the discussions of the chapter to determine whether the objectives of the chapter have been fulfilled. The researcher also introduces the discussion of Chapter 7.

## **6.2 Step 1: Establish a Theory**

As seen above, the first of the seven steps of the survey conducting method is to establish a theory. The theory should be based on the broader problem, which is being investigated, as part of the research study. Therefore, the researcher is required to review the background information on the problem area of the research

study, and to establish a theory to validate the research problem (Olivier, 2009, p. 79).

Thus, the literature on information security governance, information security requirements and SMMEs was reviewed, as discussed in Chapter 2, Chapter 3 and Chapter 4, respectively. The problem statement of this research study, pertains to the complexity of most well-known information security best practices and standards, thereby posing a challenge to their use in SA SMMEs (see section 4.9 of Chapter 4). In particular, the unique characteristics of SMMEs make the information security best practices and standards so much more complex, as discussed in section 4.6 of Chapter 4.

Therefore as seen in Chapter 4, the researcher established [from the literature] the core elements of an information security artefact developed for SMMEs. Thus, the theory to be validated by this survey is that SA SMMEs have similar characteristics to those SMMEs reported on in most of the international literature about the complex nature of information security best practices and standards (see section 4.6 of Chapter 4). Therefore, the established core elements of an information security artefact developed for SMMEs, are also necessary in the SA SMME context.

The second step of the seven step survey conducting method, is to formulate a hypothesis about the theory. Step 2 of the survey conducting method is discussed in the next section, below.

### **6.3 Step 2: Formulating a Hypothesis**

The Oxford Mini School Dictionary (2007, p. 290) defines a hypothesis as a suggestion or argument that has been made without any evidence to prove that it is true. The hypothesis typically proposes an idea about the cause of the phenomenon described in the theory.

The theory to be proven by conducting this survey, is that the core elements of

an information security artefact for SMMEs as established from the literature, are valid for SA SMMEs too. Previously published literature on the research problem, as presented in Chapter 4, all relate to studies conducted on SMMEs in countries outside SA. Therefore, it is hypothesised that SA SMMEs have similar characteristics to those of their counterparts in other countries, as discovered from the literature. As seen in section 5.6.2 Myers (1997) defines this process of validating already discovered knowledge in a different context as triangulation.

Thus, the data were collected from SA SMMEs, to test the hypothesis of this survey, thereby validating the theory proposed in section 6.2. The following section of this chapter discusses how a sample of SA SMMEs was chosen for the data collection purposes.

## 6.4 Step 3: Selecting the Sample Population

As reported in section 5.7.2 of Chapter 5, surveys observe a large population, often making it difficult to collect the data from every member of the population (Gable, 1994). Therefore, the data is collected from the sample population and is analysed to discover findings that are generalised to the larger population of the research study (Olivier, 2009, p. 81; Rattray & Jones, 2007). Although responses were not received from a large enough sample population to generalise the findings of this survey to all SA SMMEs, this section will describe the steps taken by the researcher in calculating the required sample population size. Step 4 will describe how the researcher implemented the sampling method described below, in attempting to reach the sample population. Step 5, will discuss the alternative method (to statistical inference), used to represent the findings of this survey.

The general population of interest for this survey was SA SMMEs. Thus, the characteristics of the population were, as defined in section 4.3 of Chapter 4 (turnover of less than 50 million rand, less than 200 full-time employees and gross assets valued at less than 18 million rand), according to the criteria of the NSBA (1996, p. 15). According to the Bureau for Economic Research (BER), more than

2 million (2 251 821) SA enterprises matched those criteria (were identified as SMMEs) in the second quarter of the year 2015 (BER, 2016, p. 1).

Thus, it was concluded that for this survey the general population of the survey should consist of 2 251 821 SA SMMEs. As time and other resource constraints would not allow the researcher to collect the data from each member of the population, a survey was seen as the most applicable research method. Furthermore, the ability of survey research to generalise findings from a sample population made it the most appropriate research method. Thus, the required sample population size was calculated based on the number of SMMEs in SA.

With the use of a sample size calculator (Creative Research Systems, 2012), the required sample size was calculated. The calculator used allows a minimum confidence level of 95 per cent. At a 95 per cent confidence level, the **required sample population of SA SMMEs was calculated to be 384 respondents**. The confidence interval used for the calculation was five percent.

The confidence interval is a measure of the possibility that the general population would make the same selection of an answer, as the sample population. In the context of this study, if 60 per cent of the sample population selected an answer then a confidence interval of 5 per cent would indicate that between 55 per cent (60-5) and 65 (60 + 5) of the general population agree with the answer selected by members of the sample population. The wider the confidence interval that the researcher is willing to accept, the greater the range of the entire population included in the possible selection of an answer (Creative Research Systems, 2012).

No mathematical, or statistical calculations were used to determine the confidence interval of this survey. However, a wider confidence interval decreases the number of members required in the sample population. A smaller sample population, however, means that the obtained results are not as accurate a reflection of the entire population. Thus, the researcher attempted to remain in a neutral position, by selecting the confidence interval on a one-to-ten scale.



The confidence level, on the other hand, is an indicator of the accuracy of a selection. In the example above, a 95 per cent confidence level would indicate that the researcher can be 95 per cent sure that between 55 per cent and 60 per cent of the entire population would indeed have selected that answer (Creative Research Systems, 2012).

Olivier (2009, p. 80) reports that random sampling should be used to allow all members of the population an equal opportunity to participate in the survey. Thus, the researcher attempted to distribute the survey through organisations that have close affiliations with SMMEs in SA, as discussed in the section to follow.

## 6.5 Step 4: Collecting the Data

The fourth step of the survey conducting method, involves preparing the data collection tool and distributing it to the potential respondents (Olivier, 2009, p. 81). One of the most widely used survey data collection tools is a questionnaire. Questionnaires are reported to be a standardised method of asking human respondents of the survey, for their opinion on the topic of investigation (Olivier, 2009, p. 81; Rattray & Jones, 2007; Gable, 1994).

The questionnaire used a mixture of open-ended and closed-ended questions, which had a number of nominal and Likert-scale measures in the answer-set options. Open-ended questions allow respondents to offer answers in a format which they see fit. While, closed-ended questions restrict the respondent to selecting an answer from the provided set of possible answers. Additionally, nominal measures allow the respondents to select multiple answers in closed-ended questions, with no particular order of hierarchy in the possible answers. An example from this survey, is respondents selecting the various categories of information security measures that are used in their enterprises. Likert-scale measures, are used to specify the degree to which a statement applies to the respondent. As an example, the respondents were asked to indicate how much they agreed or disagreed with a particular statement. A scale was given, with numbers representing the various

degrees of agreement or disagreement (Olivier, 2009, p. 83).

The questionnaire content was taken from various literature sources, reviewed as part of the literature review in the previous chapters. Some of the seminal works reviewed included the National Small Business Act (NSBA) of 1996, ISO/IEC2700X, NIST SP800-53 R4 and the Bureau for Economic Research's Research Note of 2016. The aim of the questionnaire was to confirm the theory as defined in a previous section of this chapter. For this reason, contributing elements included the perspective of published works, relating to information security requirements. The criteria of an information security requirement, as defined by information security best practices and standards was also included in the questionnaire. Finally, the characteristics of SA SMMEs, as defined by the National Small Business Act of 1996, as well as other constraints and challenges faced by SMMEs, were also included.

The researcher then enlisted the guidance of the Nelson Mandela University's (formerly Nelson Mandela Metropolitan University) Statistical Services Department. Guidance from this department included question wording, scales of measurement for answers, ordering questions and answers and reviewing the questionnaire length. Numerous meetings were held with consultants from this department, with the intention of a follow up meeting to analyse the collected data. With regard to the questionnaire development, a few recommendations were made and the necessary amendments to the questionnaire were made by the researcher. The amended questionnaire was then resubmitted to the statistician, who confirmed the reliability and accuracy of the tool to collect the required data.

Figure 6.1, below, is a snapshot of an email from the statistician, with recommendations to improve the questionnaire. Additionally, the statistician confirms the adequacy of the questionnaire to collect the required data. All the recommendations were implemented before distributing the questionnaire. The questionnaire, is attached to this dissertation, as Appendix B.

I have the following recommendations;

1. Question 12 asks the respondent to choose all challenges that the organization faces AND give examples of how the challenges affect implementation. I would suggest that you ask the participant to give examples after choosing the challenges. I.e. Move that sentence to after "e. Other (please specify)".
2. "Please provide motivation for your answer" on Question 14 should be moved to below "c. I do not know".
3. "If yes, please give a brief description of this system. If no, please state why not" on Question 16 should be moved to below "c. I do not know".

Another suggestion is that you keep your wording consistent when asking for motivation/elaboration of an answer. However, this is entirely up to you. The content of the questionnaire is adequate for answering your research questions.

Figure 6.1: Snapshot of statistician email of recommendations

A pilot study was conducted with the post-graduate students at the Nelson Mandela University's Centre for Research in Information and Cyber Security (CRICS). Eleven post-graduate students were contacted via electronic mail; but only four responses were received. The purpose of a pilot study is not to produce results that are generalisable, but to identify misunderstood questions, unexpected responses, even places for which the researcher did not allow enough space with unexpectedly long answers. Therefore, the final version of the questionnaire should be tested by using a pilot study. In addition, the population used for a pilot study need not be randomly selected (Olivier, 2009, p. 84).

Thus, the post graduate students of the CRICS, with their advanced understanding of information security [compared to those with no information security knowledge] could focus more on queries related to the questionnaire design. The same online survey for the distribution of the questionnaire, was used for the pilot study. All the potential participants were sent an Excel spreadsheet with the questions, the objective of each question, and the source of each question, along with the final version of the questionnaire. The participants then had to submit their recommendations by using an online form, similar to that used in the final questionnaire. To avoid any personal or emotional vendetta, all responses were submitted anonymously. Most of the responses included recommendations

on attending to grammatical errors.

Figure 6.2 is a snapshot of a few of the suggestions made in the pilot study.

**Suggestion 1:** Perhaps make the question 1 with a cap letter: Question 1

**Suggestion 2:** If you answered yes to question 1, which South African province is your organisation or head office of your organisation situated in? Remove "the" before head office

**Suggestion 3:** I would of said; "Which of the following influences the selection of information security controls deployed by your organisation."

**Suggestion 4:** On the PDF version I do not see a specific space provided for the respondents to "give a few examples".; ; Also I would separate the question into two sentences to make it easier to read.; ; "Choose all challenges which your organisation faces in implementing information security. Give a few examples of how these challenges affect its implementation."

Figure 6.2: A snapshot of several suggestions from the pilot study

After correcting the identified anomalies in the questionnaire, by implementing the suggestions from the pilot study, the final version of the questionnaire was published. E-Survey Creator, an online survey tool, was used to publish the final version of the questionnaire. This online survey tool was specifically chosen, as it allowed students with a valid Nelson Mandela University email address, free access to the full suite of features provided by the survey tool.

The survey tool was used to officially publish the questionnaire and the URL to the questionnaire was distributed via email on the 22nd of May, 2017. More than 15 small business related growth and development incubation hubs and agencies, magazines, forums (organisations affiliated to SA SMMEs) and several individual SMME owner/managers were contacted. The researcher used these means of distributing the survey URL, as it presented a central, simple and inexpensive (convenient) manner to contact the target population. The agencies, magazines, forums and owner/managers were promised that all responses were completely

anonymous and that they could receive the findings of the study, if they wished to do so.

These agencies, magazines and forums were asked to forward the link to any SMMEs in their database, with no legally binding obligations; as participation was voluntary and up to the SMMEs themselves. Telephonic invitations, permission letters and short message services (sms) messages were all used to try and garner responses. Due to a low response rate, the survey was available for longer than it was initially intended and it was only closed on the 25th of September, 2017. A copy of the letter of invitation to participate in the study, as well as of the sms messages sent, are attached as appendices.

Upon closing the survey on the 25th of September, 2017, the researcher realised that the number of responses had not reached the required sample population size. An analysis of the collected data, and how the researcher resolved the issue of low responses is discussed in the next section of this chapter.

## 6.6 Step 5: Analysing the Data

At the time of developing the survey, it was not possible for the researcher to establish exactly how many SMMEs could be contacted through each of the small business related growth and development incubation hubs and agencies, magazines, forums (organisations affiliated to SA SMMEs), as mentioned earlier, in section 6.5. Most of the organisations were not willing to disclose any information pertaining to SMMEs with an affiliation to them. It was claimed that disclosing such information would violate the confidentiality agreements between the organisation and the SMMEs. However, it is known to the researcher that several of the said organisations that were contacted, have a national presence and might have been able to reach more SMMEs than the required number for the data to be collected from a representative sample.

A mere nine, of the required sample population (384) responses were received. The nine responses included five incomplete submissions and four fully completed

questionnaires. The four incomplete submissions had most of the selection type (closed-ended) questions complete, with the opinion type (open-ended) questions incomplete. Thus, the researcher was still able to consider and analyse this section of the incomplete questionnaires, to provide insight into the knowledge of the participants on the problem at hand. The four, complete submissions provided insight into the knowledge of the participants through the selection type of questions. Understanding of the problem investigated by this research study, was garnered through the analysis of the opinion-type questions.

The following section of this chapter will discuss how the researcher ensured that the responses received were from the representatives of SA SMMEs.

### **6.6.1 Filtering the Results**

As mentioned in section 6.2, the survey focused on SMMEs in SA. Therefore, filtering questions were used to ensure that the responses received were indeed from SMMEs in SA. Several closed-ended questions were used to ascertain that the respondents were indeed representative of a SA SMME. These included firstly, whether or not the enterprise or its head office was located in SA. Secondly, the number of paid full-time employees of the enterprise, and thirdly, what the average annual revenue of the enterprise was. To assist in categorising the various enterprises, according to the size of enterprise, the respondents were also asked to indicate the economic sector or sub-sector in which they operate. Examples of the economic sectors included agriculture, mining and quarrying, manufacturing and construction, to name a few.

Nine of the respondents reported that their enterprises, or the head office, were located in SA. Furthermore, it was noted that eight of the nine respondents indicated that their SMMEs are located in the Eastern Cape province of SA. The remaining respondent, selected KwaZulu-Natal, as the province in which their enterprise or the head office thereof was located.

To assist in determining the categories of enterprise (micro, small, medium),

to which the respondents belong, the researcher analysed the number of employees and the annual revenue in relation to the economic sector, in which the enterprise operates. The NSBA (The President's Office, 1996, p. 15), offers guidance on categorising SMMEs, according to a maximum threshold of annual revenue, and the number of full-time paid employees of an enterprise.

In the instance of this survey, the reported economic sectors in which the responding SMMEs operate are: media, arts and culture, healthcare services, fashion design, software engineering, electricity, gas and water, community social and personal services, ICT and business consultancy; and ICT and telecommunications. The configuration of the nine SMMEs that responded to the survey, is as listed below:

- Six of the nine SMMEs employ between zero and five full-time, paid employees. Furthermore, these six enterprises earned between R 0 and R 150 000 in revenue at the time of responding to the survey. Within the six responses, the respondents reported that their enterprises were operating in the following economic sectors or sub-sectors:

Print and Graphic Design (Media);

Arts and Culture;

Healthcare Services;

Software Engineering;

ICT and Business Consultancy; and

ICT and Telecommunications.

As seen in the NSBA (The President's Office, 1996, p. 15)(1996, p. 15), each of the enterprises as defined above fits within the category of micro enterprises. In the micro enterprises category, enterprises cannot employ more than five full-time paid employees. Additionally, in this category, the enterprise may not earn more than R 150 000 in annual revenue;

- The one SMME that reported an annual revenue of between R 401 000 and R 1 000 000, also reported employing between zero and five full-time paid employees. Additionally, the enterprise was reported to operate in the electricity, gas and water economic sectors or sub-sectors. Therefore, it was concluded that this enterprise is categorised as a small enterprise, according to the NSBA (The President's Office, 1996, p. 15). Enterprises in this category and economic sector or sub-sector, employ up to twenty full-time paid employees; and earn no more than R 4 000 000 in annual revenue. Although the respondent indicated that the enterprise employs between zero and five full-time paid employees, the annual revenue exceeds the annual revenue threshold set for micro enterprises (R 150 000);
- Another respondent, who reported that their SMME earned an annual revenue of between R 5 000 000 and R 10 000 000, also reported that their enterprise employs between eleven and twenty full-time paid employees. The economic sector, in which this enterprise operates (community, personal and social services), this qualifies the enterprise to be categorised as a medium enterprise (see NSBA (The President's Office, 1996, p. 15)); and
- The ninth respondent reported that their enterprise earned an annual revenue of between R 151 000 and R 401 000 per annum. Pertaining to the number of full-time paid employees, the enterprise employed between zero and five employees. The fashion design economic sector, in which the enterprise operates, is not listed in the NSBA (The President's Office, 1996, p. 15). However, it was found to be similar to the catering, accommodation and other trade economic sector or sub-sector. Therefore, the enterprise was categorised as a very small enterprise (categorised as a small enterprise for the purpose of this study) according to the NSBA (The President's Office, 1996, p. 15). In this category, enterprises can employ up to ten full-time paid employees and earn a maximum of R 1 000 000 in annual revenue.

Based on the findings, as discussed above, the researcher concluded that the responses consisted of six representatives of micro enterprises, two representatives



of small enterprises and one representative of a medium enterprise. It was also confirmed that all nine respondents represented SA SMMEs; and they were, therefore, eligible to be considered valid respondents of the questionnaire.

The remainder of this section will discuss the findings of the survey, according to the core elements of an artefact for SMMEs, as discovered from the literature (see section 4.10 of Chapter 4).

### 6.6.2 Scalability

As reported in section 4.10 of Chapter 4, one of the core elements of an artefact for SMMEs is scalability. It was further reported that this core element should ensure that the artefact designed and developed for SMMEs is mindful of the flexible organisational structure and constantly evolving nature of SMMEs.

The need for such a core element in an artefact developed for SA SMMEs was identified in the findings of the survey questionnaire, as discussed in this chapter. An analysis of the findings indicated that even in the small sample of obtained responses, the category of SMMEs varies. Although most respondents indicated between zero and five full-time paid employees, a few of these enterprises earned more than the threshold annual revenue for categorising them as micro enterprises, according to the NSBA (The President's Office, 1996, p. 15). Therefore, as discussed in section 6.6.1 of this chapter; of the nine respondents, six enterprises were categorised as micro enterprises, 2 were categorised as small enterprises and another enterprise was categorised as.

Table 6.1, below is a table of the various categories of SA SMMEs identified from the responses to the questionnaire. The enterprises were categorised according to the criteria of the NSBA (The President's Office, 1996, p. 15). Although two of the enterprises were categorised as small enterprises, they reported different annual revenues, as can be seen in Table 6.1.

No. of Enterprises	Category of SA SMME	No. of Full-time Paid Employees	Annual Revenue in Rands (ZAR)
6	Micro	0 - 5	0 - 150 000
1	Small	0 - 5	151 000 - 400 000
1	Small	0 - 5	401 000 - 1000 000
1	Medium	11 - 20	5 000 000 - 10 000 000

Table 6.1: A table of the various categories of SA SMMEs that responded to the questionnaire.

As can be seen in Table 6.1 above, even in a sample of only nine responses, all three of the reported categories of SMMEs, according to the NSBA (The President's Office, 1996, p. 15) were identified. The identification of all three categories of SMMEs even in such a small pool of respondents, demonstrates that it cannot be assumed that a one-size-fits-all solution would work when for SMMEs. Thus, it was concluded that the core element of scalability is indeed necessary to consider the various categories of SMMEs, when designing and developing an artefact for SA SMMEs.

The following section will discuss how simplicity was identified a necessary core element of an artefact for SA SMMEs.

### 6.6.3 Simplicity

The core element of simplicity addresses the need for the developed artefact to be simple enough, so that even a non-information security expert, such as an SMME practitioner can implement it. Four factors influenced the need for the simplicity of an artefact that is developed for SA SMMEs. These four factors are, namely: a lack of finance, a lack of proper corporate governance, a lack of time and a lack of information security expertise. The lack of information security expertise is arguably linked to the educational qualifications of the respondents.

Only three of the nine respondents indicated that they possessed a qualification in the field of ICT. The three qualifications in the ICT field included, a Bachelor

of Technology Degree in Software Development, a Bachelor of Commerce Degree in Information Systems (with Cisco Networking and related certifications) and a respondent who holds several ICT-related certifications, such as being a certified A+ Computer Service Technician among others. Other educational qualifications included two matric certificates, one grade 9 certificate, two Bachelor of Technology degrees (one in Fine Arts and the other in Fashion Design) and one Bachelor of Arts Degree.

Table 6.2 below, is a summary of the number of respondents who possessed each of the educational qualifications, as mentioned above.

<b>Educational Qualification</b>	<b>Number of Respondents with Qualification</b>
High School Certificate (Grade 9)	1
High School Certificate (Matric)	2
ICT Related Certifications only (A+, Cisco IT Essentials, etc.)	1
Bachelor's Degree (non ICT-related, Art)	1
Bachelor of Technology Degree (non ICT related, Fine Arts and Fashion Design)	2
Bachelors Degree ICT-related (B.Comm Information Systems, B.Tech IT (Software Development))	2

Table 6.2: A table of the educational qualifications of the respondents to the questionnaire.

As seen in Table 6.2 above, only three of the respondents reported were in possession of an ICT-related qualification. Although the three respondents reported that they hold ICT-related qualifications, none of them appeared to be educational qualifications in information security.

The factors that influenced the need for simplicity, were also considered as challenges to SA SMMEs implementing information security. When asked about the challenges, the leading selection (biggest challenge) was a lack of finance (nine

selections). The second biggest challenge was a lack of information security expertise in the enterprise (five selections). A lack of proper corporate governance (four selections) and a lack of time were reported as the third and fourth challenges, respectively.

The graph below (Figure 6.3), graphically represents the challenges that the respondents indicated.

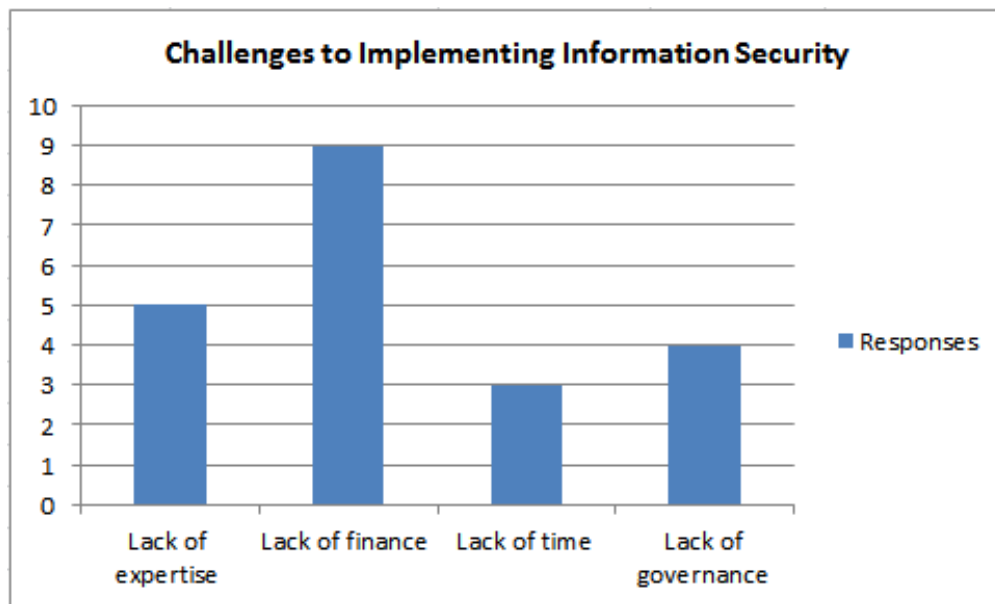


Figure 6.3: A graph of the challenges to implementing information security in respondent SMMEs

Based on the findings of the survey, as discussed above, it was concluded that an artefact developed for SA SMMEs should be simple enough to implement even where time, finance, expertise and corporate governance present a challenge to the implementation of information security. Furthermore, SMMEs reportedly need to respond quickly to customers' demands. Therefore, the simplicity of artefact developed for SA SMMEs should not hinder the ability of an enterprise to quickly respond to customers' demands.

The next section discusses the findings of the survey on the need for feasibility,

as one of the core elements of an artefact developed for SA SMMEs.

#### 6.6.4 Feasibility

The previous section discussed the need for an artefact developed for SA SMMEs, to incorporate the core aspect of simplicity. The motivators for simplicity included the challenges that SA SMMEs face, when implementing information security. In particular, four challenges were identified; and these were: a lack of finance, a lack of information security expertise, a lack of proper corporate governance and a lack of time.

This section further discusses the difficulty that SA SMMEs face in implementing information security due to the above mentioned challenges. The participants were asked whether they do make use of information security best practices and standards such as ISO/IEC27002. Only four responses were received to this question. All four respondents indicated that they do not make use of any information security best practices or standards.

A follow up question enquired about the reason for these enterprises not using information security best practices and standards. Three of the respondents reported that in their experience, information security best practices and standards are too resource intensive to be used by their enterprises. The fourth respondent claimed that their experience resulted in the conclusion that information security best practices and standards are too complex to understand in their current format.

Figure 6.4 below, is a graph of the frequency of responses, as discussed above. As mentioned above and seen in the graph, only four responses were received for this part of the questionnaire.

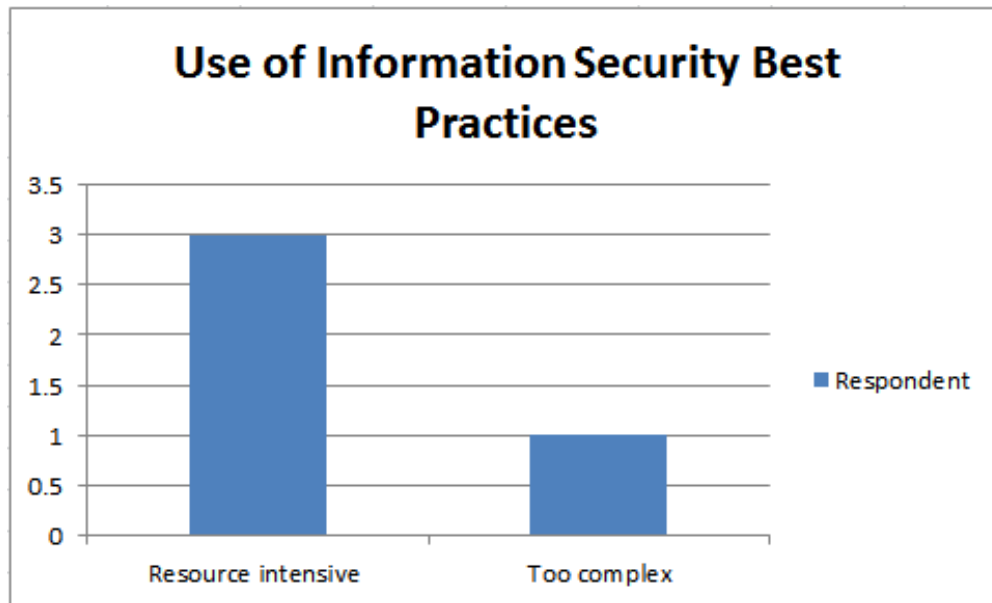


Figure 6.4: Graph of the Use of Information Security Best Practices and Standards in some SA SMMEs

Guided by the findings on the use of information security best practices and standards in SA SMMEs, as seen above, it was concluded that an artefact developed for SA SMMEs should not be too resource intensive or too complex in any form. Nevertheless, much benefit could be drawn from an artefact, which seeks to make the use of information security best practices and standards simpler and more feasible.

Expanding further on the benefit of an artefact developed for SA SMMEs, the next section discusses the need for utility as one of core elements of such an artefact.

### 6.6.5 Utility

The core element of utility addresses the need for an artefact developed for SMMEs, to be fit-for-purpose. In this context fit-for-purpose indicates that the artefact should be appropriate for the size and level of maturity of an enterprise.

It was reported in section 4.7 of Chapter 4 that most SMMEs have a flat or owner-manager centric corporate governance management structure. This discovery was found to be true for SA SMMEs too, by means of the survey. The participants in the survey were shown a three-tier corporate governance management structure, as seen in Figure 2.2.1 in section 2.2.1 of Chapter 2. The participants were then asked to indicate whether or not the three-tier corporate governance management structure represents the corporate governance structure of their enterprise also.

Three of the four respondents indicated that the three-tier corporate governance management structure does represent the corporate governance management structure of their enterprise. The remaining respondent stated that they are unsure whether or not their enterprise has a similar corporate governance management structure.

Expanding on the corporate governance management structure of the SMMEs, the participants were asked which of the management levels are present in the management decisions of the enterprise. Two of the four respondents indicated that strategic-level management and tactical-level management participated in the decision-making within their enterprises. The other two respondents claimed that all three (strategic, tactical and operational) levels of management participated in the decision-making within their enterprises.

Based on the findings of the survey, it became evident that SA SMMEs have varying corporate governance management structures. The corporate governance management structure of an enterprise can commonly be linked to the level of maturity of that enterprise. This is generally true; as enterprises with more employees often have a three-tier corporate governance management structure (see Chapter 4 section 4.7); while enterprises with fewer employees have a more flat corporate governance management structure. Thus, the research concluded that the core aspect of utility is indeed necessary when developing an artefact for SA SMMEs.

The following section will discuss the findings of the survey regarding the transparency between the various corporate governance management levels in the decision-making. Furthermore, the section will also discuss the findings pertaining to the alignment of information security controls to the information security requirements of an enterprise.

### **6.6.6 Transparency**

The core element of transparency, as seen in section 4.10 of Chapter 4, refers to transparency in the corporate governance decisions within an enterprise. This includes decisions made pertaining to the governance of information security within the enterprise (section 2.2 of Chapter 2).

Therefore, the participants of the survey were asked if their enterprises make use of an ISMS; as a structured method for information security management decisions within their enterprises. All four of the responses indicated that their enterprises do not make use of an ISMS. More so, only one of the participants claimed to implement another form of decision-making system. This participant claimed that their enterprise has a quality management system in place.

However, even a quality management system shows no direct connection to an information security decision-making system. Thus, it was not surprising that all four responses indicated that the information security controls implemented in these enterprises do not have a clear link to a higher level of management decisions. This could also be interpreted as the implemented information security measures not being aligned with the vision and objectives that strategic management has for the enterprise. Interestingly enough, it was observed that all four respondents indicated that it is indeed important for the implemented information security measures to be linked to a higher level of management decisions.

Although all four participants indicated that they were aware of the need to align the implemented information security measures with the decisions taken by the higher level management of an enterprise, none of the participants reported



doing so. This could be attributed to the difficulty that the participants reported in establishing their information security requirements.

As seen in Figure 6.5, the majority of the respondents (3) reported that it is moderately hard for them to establish information security requirements that link to the vision and objectives of the enterprise. One of the participants reported that it was in fact very hard to perform this task.

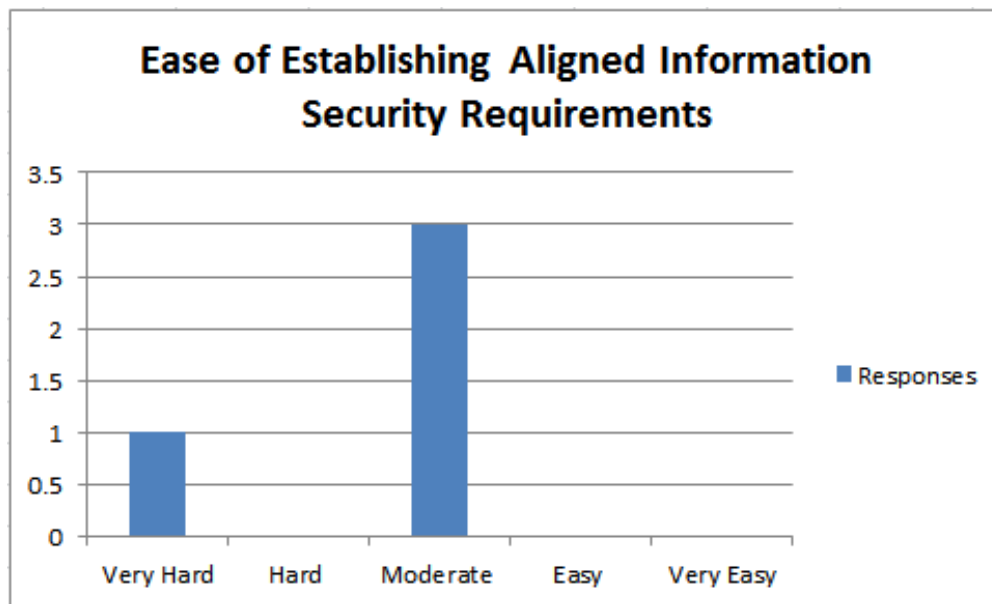


Figure 6.5: A Graph of the Ease of Establishing Information Security Requirements in some SA SMMEs

Based on the findings of the survey as discussed above, the researcher concluded that transparency is currently not evident in the decision-making processes of SA SMMEs. Therefore, it is imperative that an artefact be developed for SA SMMEs to promote transparency in decision-making, among the corporate governance management levels of the enterprise.

The next section of this chapter discusses the findings of the survey pertaining to executive management insight into how information security risks are managed in the enterprise.

### 6.6.7 Risk Control

Similar to transparency, risk control requires that the executive management of the enterprise has insight on the decisions made regarding the control of information security risks. Therefore, this core aspect requires that a clear path is shown from the process of identifying information security risks, to the selection of information security controls to protect the information asset at risk.

As discussed in the previous section, responses from the survey indicated that most implemented information security controls were not aligned with the information security requirements of the enterprise, or to a decision taken by higher (strategic) level management. Furthermore, it was discovered that in most of the enterprises, the selection of information security controls is based on past experiences of the SMME owner-manager.

As seen in Figure 6.6 , there were four selections made by the nine respondents. Firstly, six of the respondents indicated past experiences. Secondly, one respondent stated that there was no information security or that it was implemented only when needed. Thirdly, another claimed that the objectives of the enterprise informed the selection of information security measures. Fourth and finally, another respondent claimed that the information security measures implemented in the enterprise were chosen from observing what their competitors do.

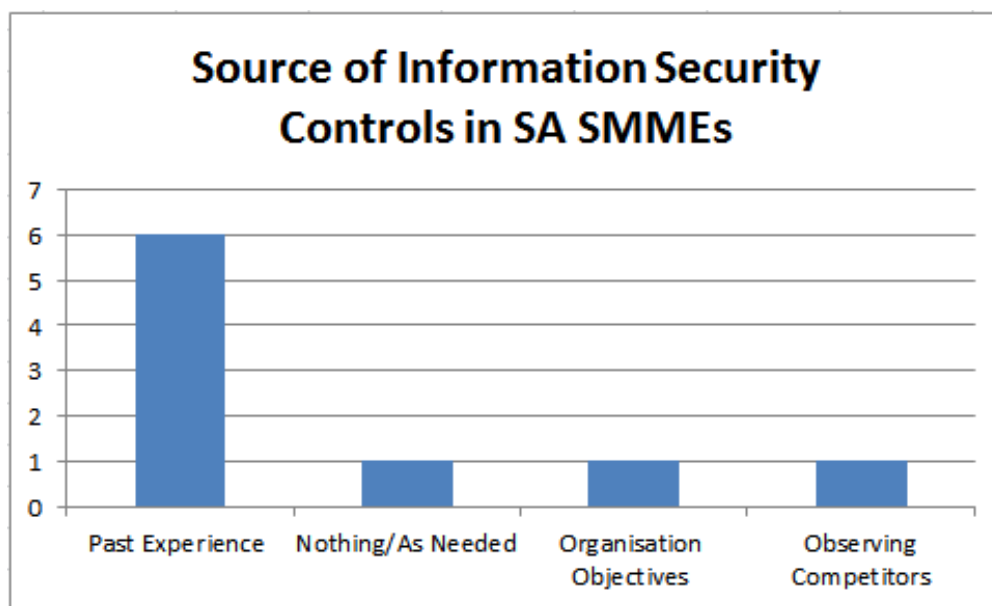


Figure 6.6: A Graph of the Source of Information Security Controls in some SA SMMEs

Based on the findings of the survey, as discussed above, it was concluded that currently there is no clarity or executive management insight on how information security risk is managed or how information security controls are selected in some SA SMMEs. Thus, an artefact developed for SA SMMEs should be mindful of the current lack of risk control in these enterprises.

This section concludes the discussion of findings based mainly on the questionnaire responses to the selection type (closed-ended) questions. The following section will briefly discuss the recommendations and the suggestions offered by the respondents of the survey.

### 6.6.8 Further Discussions

As mentioned in the previous section, the participants were offered the opportunity to present a few recommendations and suggestions, as input to the development of the artefact. The recommendations and suggestions were collected by means of

open-ended questions. Two questions were used to collect the recommendations and suggestions from the respondents. Firstly, the respondents were asked to elaborate on how a model developed for SA SMMEs could assist in determining the information security requirements of the enterprise. To this question, the respondents replied that such a model would simplify the process of establishing the information security requirements of the enterprise especially where the owner-manager of the enterprise does not possess the necessary expertise. Furthermore, in order for the benefit of the model to be realised, the selected users would require specific training in using the model.

Secondly, the respondents were asked to make suggestions on what a researcher should consider, when designing a model to be used by SA SMMEs. The consensus was that the model should be simple enough to understand and implement in an environment in which information security expertise is scarce. And particularly because most SMME owner-managers are specialists in their field; and they might not have any ICT or information security knowledge. It was also included that the researcher should consider that most SMMEs were too small to have more than one layer of management within the corporate governance management structure of the enterprise. Thus, simplicity and scalability are essential to the user friendliness of a model for SA SMMEs.

This concludes the discussion on the results and findings on the survey. The following section re-evaluates the hypothesis formulated in Step 2 of the survey conducting process.

## **6.7 Step 6: Re-evaluating the Hypothesis in Comparison with the Survey Results**

The sixth and seventh steps of the survey conducting process are about determining the correctness of the hypothesis, based on the findings of the questionnaire. The seventh step of the process involves confirming or rejecting the theory. This section

of the chapter re-evaluates the hypothesis established in Step 2 of the survey conducting process.

As mentioned in Step 2 of the survey conducting process, it was hypothesised that SA SMMEs have similar characteristics to those of their counterparts in other countries, as discovered from the literature. An analysis of the data gathered through the survey revealed that some SA SMMEs also have a flat corporate governance management structure, similar to those of most other SMMEs, as reported by the literature in section 4.7 of Chapter 4.

Furthermore, SA SMMEs do not have the financial resources or the information security expertise to implement most well-known information security best practices and standards, similar to their counterparts, as seen in section 4.9 of Chapter 4.

The need for simplicity, feasibility and scalability are all attributed to the corporate governance management structure common to SMMEs and the lack of resources in these enterprises. Utility was proven to be necessary to ensure that the artefact matures together with the rapidly evolving enterprise; as SA SMMEs are faster growers much like their counterparts, as discovered from literature.

Another similarity between SA SMMEs and their counterparts, as seen in the literature, is the ad hoc or reactive implementation of information security controls (see section 4.8 of Chapter 4); thus, emphasising the need for transparency risk controls, as core aspects of an information security artefact developed for SA SMMEs.

Therefore, the researcher concluded that the hypothesis of this survey as established in Step 2, was proven to be true. SA SMMEs do indeed have similar characteristics to their counterparts as can be seen in the literature. The next section will review the validity of the theory established in Step 1 of the survey conducting process.

## 6.8 Step 7: Confirm or Reject the Theory

Step 7, the final step of the survey conducting process, entails confirming or rejecting the theory established in Step 1 of the process. The theory established for proof through this survey, is that *SA SMMEs have similar unique characteristics to their counterparts, as observed in the literature (see section 4.6 of Chapter 4). Therefore, the established core elements of an information security artefact developed for SMMEs, are also necessary in the SA SMME context.*

As seen in Step 6, the hypothesis of this survey proved to be true, thus confirming that SA SMMEs do indeed have similar characteristics to those of their counterparts, as seen in the literature. Therefore, it can be concluded that the core elements of an information security artefact developed for SMMEs as discovered from literature, are necessary in the SA SMME context too. In simpler terms, it was proven that an information security artefact developed for SA SMMEs should also include the core elements of an artefact developed for SMMEs, as seen in section 4.10 of Chapter 4.

The next section of this chapter briefly mentions the limitations, which prevented the findings of this survey from being generalised to all SMMEs in SA.

## 6.9 Limitations of the Survey

Despite an attempt by the researcher to contact as many SA SMMEs as possible, the received responses were minimal. Although the researcher contacted more than 15 small business related growth and development incubation hubs and agencies, magazines, forums (organisations affiliated to SA SMMEs) and several individual SMME owner/managers, the required number of responses were not received. Due to this limitation, the findings of the survey cannot be generalised to all SA SMMEs. Unlike most survey participants, SMMEs are not easily identifiable; as the enterprise should fit the criteria of the NSBA (National Small Business Act)

of 1996. Therefore, it was not possible for the researcher to approach enterprises to do walk-in attempts in order to increase the survey response rate.

## 6.10 Conclusion

In this chapter, it was determined that surveys are a research method used to count the occurrence of a phenomenon in a population (a group of systems or individuals with similar characteristics). However, populations are too large to count each individual in the population. Therefore, a representative of the sample population is used to collect the data; and the findings are generalised to the entire population through inferential statistics. However, a large enough representative sample population is not available at times, making it difficult for any inferential statistics to be performed on the collected data.

Similarly, in this survey, the researcher contacted a large number of more than 15 small business related growth and development incubation hubs and agencies, magazines, forums and several individual SMME owner/managers, yet only 2.34 per cent of the required sample population responded. Therefore, the researcher resorted to using descriptive statistics to summarise the findings of the survey, in order to represent them in an easier to understand graphical appearance.

To collect the data, the researcher used an online questionnaire, which was developed by following the guidance of the survey conducting process, as suggested by Olivier (2009, p. 79). As part of the seven steps of the survey conducting process, the researcher collected the data to validate a theory by proving a hypothesis. The hypothesis of this survey was that SA SMMEs have similar unique characteristics to those of their counterparts, as may be seen in the literature.

The analysis of the data collected from nine SA SMMEs that participated in the survey, proved that SA SMMEs do indeed have similar unique characteristics to those of their counterparts, as seen in the literature. Thus, the researcher validated the theory that the core elements of an information security artefact developed for

SMMEs, as discovered from the literature, are necessary for an information security artefact developed for SA SMMEs too.

The next chapter will discuss how the findings of this survey (along with other elements) were integrated into the information security artefact, developed, in order to solve the problem addressed by this research study.



# Chapter 7

## The Alignment of Information Security Requirements

*“Discovery consists of seeing what everybody has seen, and thinking what nobody has thought.” -Albert Szent-Gyorgyi*

### 7.1 Introduction

It was discussed in the previous chapter, Chapter 6, how triangulation was used to test whether the discoveries from literature are also true in the SMME context. Furthermore, the findings of the survey confirmed that the few SA SMMEs, which participated in the survey, confirm the discoveries from the literature. Thus, the researcher was able to conclude that the discoveries made from the literature, are valid to argue towards draft principles to guide the development of an artefact for SA SMMEs.

Therefore, the objective of Chapter 7 is twofold. *Firstly, to argue towards the draft principles. Secondly, to discuss the model, which was developed as the proposed solution to the research problem identified in section 1.6.1 of Chapter 1.* A proof-of-concept prototype of an automated tool that was developed based on the model and will also be discussed in this chapter.

This chapter will begin by discussing how the draft principles were derived. A later section of the chapter will discuss why the proposed solution of this research study qualifies as a model rather than a framework. The remainder of the chapter will be discussed in two parts: PART I and PART II.

PART I, comprises a discussion of the proposed model, as the solution to the research problem. The proposed model has a *governance aspect*, as discussed in section 7.5, and a *processes aspect*, as discussed in section 7.6. While PART II of this chapter will discuss the automated tool that was developed, based on the proposed model, as discussed in PART I of this chapter. A concluding section will verify that the objectives of the chapter has indeed been accomplished.

## 7.2 Deriving the draft principles

As discussed in section 5.5 of Chapter 5, the Design Phase of the integrated research design used throughout this study, instructs the research to derive draft principles. The purpose of the draft principles was to guide the design and development of the proposed model as the artefact output by this research study. Thus, this section of the chapter will discuss the draft principles used to design and develop the proposed model. As recommended by Herrington et al. (2007), the draft principles are based on the existing knowledge, as can be seen in Table 7.1 below.

Outcomes of Effective Information Security Governance ( <i>G</i> )	SMME Artefact Core Elements ( <i>E</i> )	IS Requirements Perspective ( <i>P</i> )	Information Security Requirements Criteria ( <i>C</i> )
1. Strategic alignment 2. Risk management 3. Resource management 4. Performance measurement 5. Value delivery 6. Business process convergence	1. Scalability 2. Simplicity 3. Feasibility 4. Utility 5. Transparency 6. Risk control	1. IS measurement 2. Identify appropriate IS controls 3. Suits different sizes	1. Source 1: Risk Identification 2. Source 2: Legislative Requirements 3. Source 3: Business and Information Objectives

Table 7.1: A table of discoveries from the literature review.

As mentioned above, Herrington et al. (2007) recommended that the draft principles to guide the design and development of the artefact should be based on the existing knowledge. Thus, each of the columns in Table 7.1 is populated with discoveries from a literature review that was conducted and reported on in Chapters 2 to 4. Furthermore, the findings of the survey in Chapter 6, confirmed this phenomenon in a few SA SMMEs too.

Chapter 2 presented the outcomes of effective information security governance, labelled as *G* in Table 7.1. In Chapter 3, the perspective *P* of various authors on IS requirements was discovered. Additionally, in Chapter 3, the criterion *C* of an information security requirement was discovered from information security best practices and standards. The core elements of an artefact developed for SMMEs *E*, were discovered from the literature, as discussed in Chapter 4.

Through the presentation of the discoveries, as mentioned above, the researcher argued towards the seven draft principles, as listed below. This type of argumen-

tation is known as evidential argumentation, as defined by Mason (2002, p.176); and it can be seen in section 5.7 of Chapter 5 . Although named draft principles, these should not be confused as a preliminary version of the principles. The term draft in this context refers to the use of the principles to guide the design and the development (drafting) of the proposed model.

The seven draft principles that were derived to guide the design and the development of the proposed model are as follows:

1. **Strategic alignment**- an enterprise should exhibit transparency (*E5*) on how strategic decisions, taken by the strategic-level management of the enterprise regarding information security governance, get translated into information security measures and roles and responsibilities. Therefore, the information security measures of an enterprise should be aligned with the business strategy, principles, and the business requirements of the enterprise for information processing (*C2*). In doing so, the information security measures of the enterprise will support the information security objectives of the enterprise (*G1*).
2. **Risk control**- it must be clear how decisions are made within an enterprise, to assess the risk to its information assets (*C1*), and how appropriate IS controls are selected to address this risk (*G2, P2*). Thereby, enabling the executive management of the enterprise to have insight on the decisions taken regarding IS risk management (*E6*).
3. **Feasibility**- due to the limited human resources, limited finance, limited expertise and poor infrastructure (*E3*), the proposed model should not be resource intensive. Furthermore, where available, the IS knowledge and infrastructure of the enterprise should be utilised efficiently and effectively (*G3*).
4. **Performance measurement**- IS requirements should be used as a metric to measure the effectiveness of IS efforts (*P1*) in achieving the information processing and information security objectives of the enterprise (*G4*).

5. **Utility**- the proposed model must be fit-for-purpose (*E4*) in optimising the information security investment of an enterprise, according to the size and the level of maturity of the enterprise (*E1,P3*), to support its organisational objectives (*G5*).
6. **Simplicity**- the processes of the proposed model must be easily integrated with the processes of an enterprise (*G6*), without hindering the ability of SMMEs to quickly respond to customers' demands (*E2*).
7. **Due diligence**- an enterprise, which has implemented the proposed model should be able to show that due diligence was done. For this reason, enterprises should show that reasonable steps were taken to avoid the contravention of legal, statutory, regulatory and contractual requirements (*C3*).

Since the draft principles have been derived, as described above, the researcher will discuss how the proposed model was designed and developed, according to the seven draft principles. However, it is necessary to explain why the model proposed as the solution to this research study, is defined as a model, rather than a framework.

### 7.3 A framework versus a model

It is claimed that frameworks and models share similarities, such as both types of artefacts being defined as the basic structural idea of a design (Merriam-Webster, 2018). The similarities of the two types of artefacts often result in the terms framework and model being used interchangeably (Tomhave, 2005, p. 8). Therefore, this section of Chapter 7 will briefly discuss the definition of each of these two types of artefacts, as seen in the literature. Furthermore, the author highlights why the artefact output by this research study is indeed a model, rather than a framework.

A framework, is defined as a basic plan or structural frame that determines the shape and therefore has a direct bearing on the functioning of a system (Oxford Mini School Dictionary, 2007, p. 238; Tomhave, 2005, p. 8). While a model, holds

the definition of being a structural design that represents the essential aspects of a system, without providing any specific guidance on the functioning of the system. Therefore, a model can serve as a visual representation for imitation, or as a blueprint for developing new systems (Tomhave, 2005, p. 8; Olivier, 2009, p. 45). Although models represent processes, variables and relationships within a system, they do not offer any specific guidance on the functioning of the subsequently developed system (Tomhave, 2005, p. 8; Olivier, p. 45).

The artefact output by this research study represents the typical management structure (corporate governance structure) of SMMEs, the three main sources of information security requirements and the processes needed to determine the information security requirements, as well as the three distinct categories of SA SMMEs. Although, the artefact depicts the relationship between the categories of SMMEs and the processes, it is not prescriptive of any particular steps or methods required to conduct the process. Descriptions of what the process is intended to achieve may be provided; but no instructions or steps to conduct the process are given.

Additionally, the artefact does not provide steps or instructions on how to proceed from establishing the information security requirements of an enterprise, to the development of an ISMS or the selection of information security measures. Furthermore, the artefact offers a visual representation as a blue-print of the typical management structure within SMMEs.

Therefore, SA SMMEs can use this model as a guide to develop their own information security governance structures. However, the particular steps or procedures of developing such a structure would form part of a framework. Thus, from the justification seen above, it may be concluded that the artefact output by this research study is indeed a model rather than a framework. Part I of this chapter follows next and will briefly discuss the components of the model.

# The MAIRSS Model

## 7.4 PART I: Constructing the MAISRSS

As discussed above, the artefact developed from this research study possesses the characteristics of a model, rather than those of a framework. Thus, the developed artefact can be defined as a model. This section of Chapter 7 will discuss the procedure followed by the researcher in constructing the model.

The Model for the Alignment of Information Security Requirements within South African Small Medium and Micro Enterprises (MAISRSS) is the artefact developed by this research study as the solution to the research problem identified in section 1.6.1 of Chapter 1.

Furthermore, as seen in section 1.6.1 of Chapter 1, the research problem entailed that the current information security best practices and standards are too complex for SA SMMEs to use in determining their information security requirements. Additionally, in section 5.5 of Chapter 5, it was discussed that the design and development of the artefact output by this research study should be guided by the draft principles. Hence, the draft principles which guided the design and development of the MAISRSS were discussed in section 7.2 of this chapter.

However, before the design and development of the MAISRSS, a theoretical model was constructed, in accordance with Phase 2 of the integrated research design, as seen in section 5.7 of Chapter 5. The theoretical model was based on the information security governance model (direct/control cycle), Figure 2.2.2 in Chapter 2 by Von Solms and Von Solms (2006). Also contributing to the theoretical model, were the three sources of an information security requirement, as identified in section 3.2 of Chapter 3. The purpose of the theoretical model was to provide SA SMMEs with a blueprint structural guide to establish their unique information security requirements that are aligned to the business principles and objectives for information processing.

As can be seen in Figure 7.1 below, the theoretical model refers to a three-tiered corporate governance management structure. However, it was discussed in section



4.7 of Chapter 4 that most SMMEs typically resemble a flat CEO-owner-centric corporate governance management structure. The flat CEO-owner-centric corporate governance management structure was confirmed through a survey conducted on a few SA SMMEs, as reported in Chapter 6.

A well-established scholar, Alfred Korzybski, once wrote *“If the map shows a different structure from the territory represented, then the map is worse than useless, as it misinforms and leads astray”*. Therefore, to accurately represent the SMME corporate governance management structure, the MAISRSS was developed according to the corporate governance management structure typical of most SMMEs (see Figure 7.3).

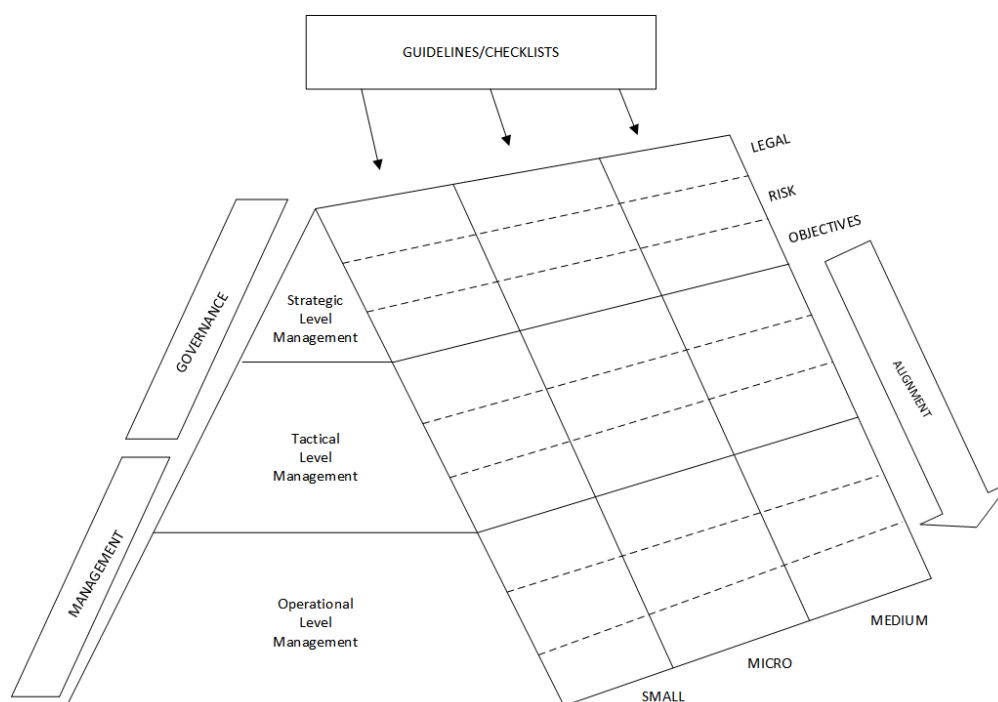


Figure 7.1: The Theoretical Model for the Alignment of Information Security Requirements within SA SMMEs

The draft principles, as discussed in section 7.2, not only reshaped the corporate governance management structure of the model; but they also changed the

proposed method for SMMEs to determine their unique information security requirements. In the MAISRSS (Figure 7.2), processes are proposed for SMMEs to determine their information security requirements, unlike the checklists or guidelines of the theoretical model (Figure 7.1).

The MAISRSS maintains the inter-tier and intra-tier communication between the corporate governance management levels, as defined by the NIST SP800-53 R4 (2013) (see Figure 5.5). As seen in Figure 7.2, arrows are used to indicate how the three corporate governance management levels (strategic, tactical and operational) communicate. Furthermore, a vertical arrow is used to depict how CEO-owner-centric decision making is in SMMEs. This is logically explained by considering that an SMME with fewer employees (smaller), is more reliant on the key actor (the CEO or owner) to make most of the decisions within the enterprise.

Also seen in Figure 7.2, a horizontal arrow at the bottom of the figure depicts how the number of processes for an SMME to determine its information security requirements increases with the size and the category of enterprise (small, medium or micro).

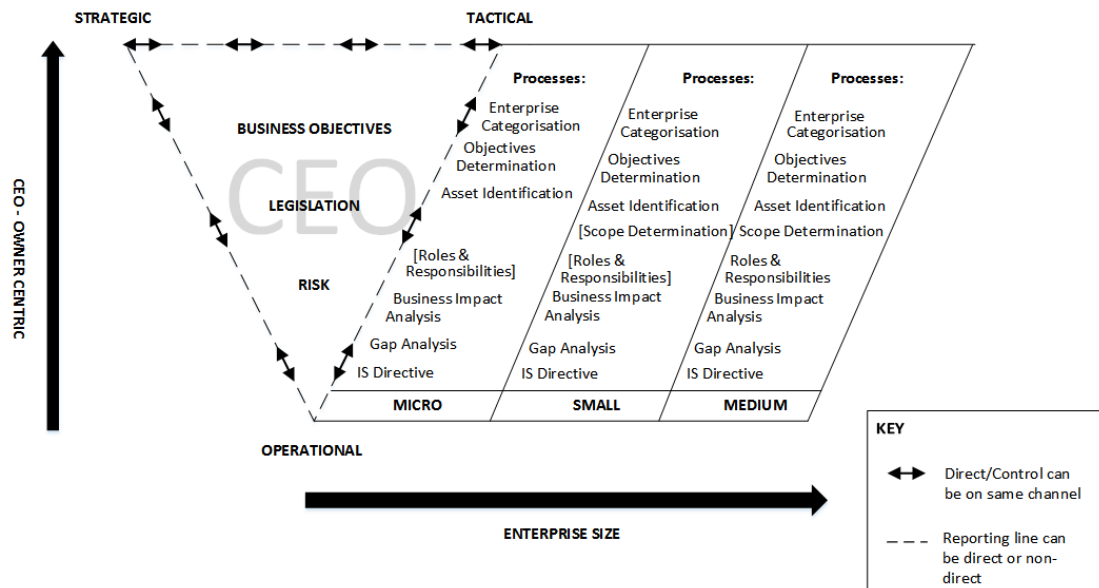


Figure 7.2: Model for the Alignment of Information Security Requirements in SA SMMEs

The specific components of the governance aspect of MAISRSS will be discussed in the next section of part one of this chapter.

## 7.5 The Governance Aspect

As mentioned in section 7.4, it was discovered that the theoretical model, which was constructed, did not accurately represent the flat CEO-owner-centric corporate governance management structure typical of most SMMEs. Therefore, it was concluded that the governance aspect of the MAISRSS should attempt to provide a more accurate representation of the flat CEO-owner centric corporate governance structure. The MAISRSS governance aspect features the flat CEO-owner-centric corporate governance management structure, as seen in Figure 7.3 below. This section of the chapter will discuss how the governance aspect of the MAISRSS

attempts to present a more accurate description of the flat CEO-owner-centric corporate governance structure typical of most SMMEs.

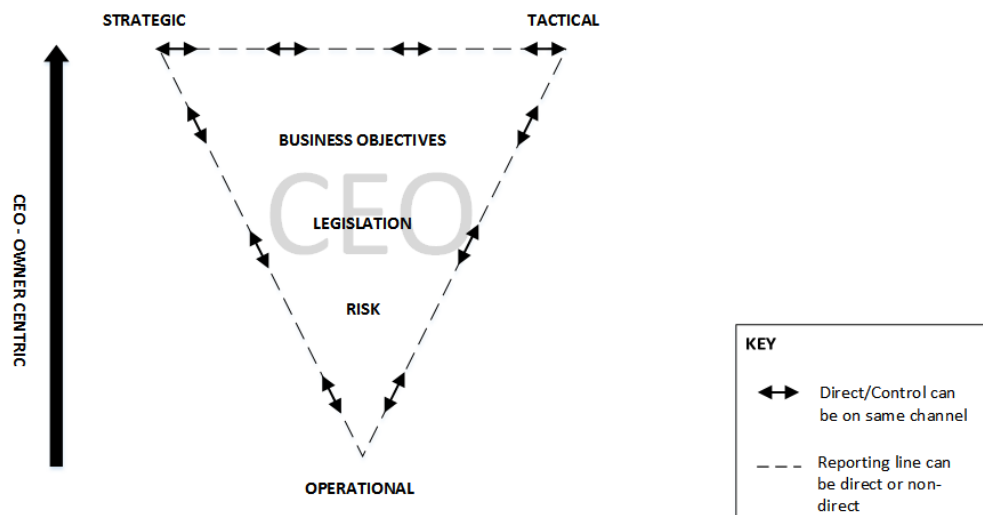


Figure 7.3: The Governance Aspect of the MAISRSS

The governance aspect of the MAISRSS, as seen in Figure 7.3, was constructed based on the guidance of the seven draft principles derived in section 7.2 of this chapter. As discussed in section 7.4, a survey was used to confirm the typical corporate governance management structure of a few SA SMMEs. According to the findings of the survey, the typical corporate governance management structure was confirmed as being the flat CEO-owner-centric corporate governance management structure, as reported in the literature (see Chapter 6). Thus, it was concluded that the flat CEO-owner-centric corporate governance management structure, as seen in the governance aspect of the MAISRSS, provides an accurate representation of the typical corporate governance management structure common to most SA SMMEs.

In the flat CEO-owner-centric corporate governance management structure,

the same individual (CEO-owner), who is responsible for most tasks within the organisation, also performs all of the corporate governance tasks. Therefore, it is reported that the existence of the organisation is dependent on the CEO-owner (Beaver & Prince, 2004; Hankinson et al., 1997). However, Levy (2009) reports that SMMEs and their organisational structures are constantly evolving. Therefore, the corporate governance management structure of these enterprises also constantly evolves. Thus, to provide utility to SMMEs, the governance aspect of the MAISRSS should also be appropriate to the size and maturity of the SMME, even as it develops (ACCA, 2015, p. 4).

Hence, the governance aspect of the MAISRSS includes the three corporate governance management levels typical of most organisations. These are: the strategic-level management, the tactical-level management and the operational-level management, as discussed in section 2.2.1 of Chapter 2.

An upward pointing arrow to the left of the governance aspect triangle, indicates how decision-making becomes CEO-owner-centric with the fewer management levels (closer to strategic-level management). The downward facing triangle indicates that in SMMEs, the tactical-level and the strategic-level management can be on the same level (filled by the same individual); whereas, the operational-level management is always at a lower level.

On the inside of the governance aspect triangle, are the three sources (criterion) of information security requirements. As listed in section 3.2 of Chapter 3, information security requirements stem from three main sources that are unique to the characteristics and the constraints of an enterprise and its information assets (ISO/IEC27002, 2013, p. vi; Gerber & von Solms, 2008).

Hence, the three sources of information security requirements appear at the centre of the MAISRSS governance aspect, as seen in Figure 7.3. The order in which the three sources of information security requirements appear in MAISRSS is of particular interest. Business objectives, which are influenced by the directives from the strategic-level management, have an influence on the operations of the

enterprise; and therefore, also on the legislation applicable to the enterprise. In turn, information security risks can affect the compliance of an enterprise with legislation; and they can potentially be of major cost to the enterprise, depending on the liability placed on the enterprise by the legislation; thus, forming the upside-down pyramid of the three sources of information security requirements.

In the event of more than a single individual assuming the various corporate governance management levels within an SMME, dashed lines were used, as seen below in Figure 7.4. The dashed lines indicate that the role of management at all levels could be performed by the same individual (common in the smallest organisations). Alternatively, the roles at the various management levels can be performed by different individuals, which is commonly seen in larger organisations (see section 4.7 of Chapter 4).

Furthermore, to maintain the inter-tier and the intra-tier communication between the corporate governance management levels, as seen in Figure 5.5 of Chapter 5, bi-directional arrows were used. The bi-directional arrows indicate how each of the three corporate governance management levels in SMMEs can communicate with each other directly, unlike in the three tiered corporate governance management structure typical of most large organisations. The bi-directional arrows are also seen in Figure 7.4 below.



Figure 7.4: The Direct/Control Lines of SMMEs

For explaining how the governance aspect of the MAISRSS provides utility in being scalable to the size and maturity of an SMME, an example will be used. In this example, the same individual within the SMME acts as both, the strategic-level management and the tactical-level management. In other words, these roles are not distinctly defined within the enterprise. Whereas, the role of operational-level management is performed by a different individual.

It therefore appears to be logical that the communication between the strategic-level management and the tactical-level management is direct in both ways (bi-directional), as these management levels are occupied by the same individual. In a similar manner, the operational-level management can communicate directly with both the strategic-level management and the tactical-level management of the enterprise. Therefore, it is also logical to conclude that the direct and the control functions within the enterprise are not propagated and cascaded through a three-tiered corporate governance management structure, as discussed in section 2.2.1 of Chapter 2.

Rather, the direct and the control functions take place through a direct two-way communication between the three corporate governance management levels.

To simplify the establishment of information security requirements, MAISRSS has lists of processes that SMMEs should complete. These lists of processes are discussed in the following section of this chapter.

## 7.6 The Process Aspect

A process as defined by the Oxford Mini School Dictionary (2009, p. 465), as “a series of actions for making or doing something”. The processes presented by MAISRSS are indeed a series of actions for SA SMMEs to determine their unique information security requirements. As discussed in section 3.2 of Chapter 3, information security requirements stem from three sources and are unique to the characteristics and constraints of the organisation.

Furthermore, information security requirements are fundamental to the development of an ISMS within any organisation (Asosheh et al., 2013). According to Calder (2009, p. 35), the scope of an ISMS is relative to the size of the organisation. In particular, it is reported that the smallest organisations should have an ISMS scope that encompasses every aspect of the organisation. While, larger organisations, are reported to select only the most critical business assets and departments to include in the ISMS scope. Thus, MAISRSS, categorises the SMMEs in order

to offer guidance in selecting the processes which are most appropriate for the size and category of the SMME. Figure 7.5 below, is a snapshot of the processes aspect of the MAISRSS.

**MAISRSS THE PROCESSES ASPECT**

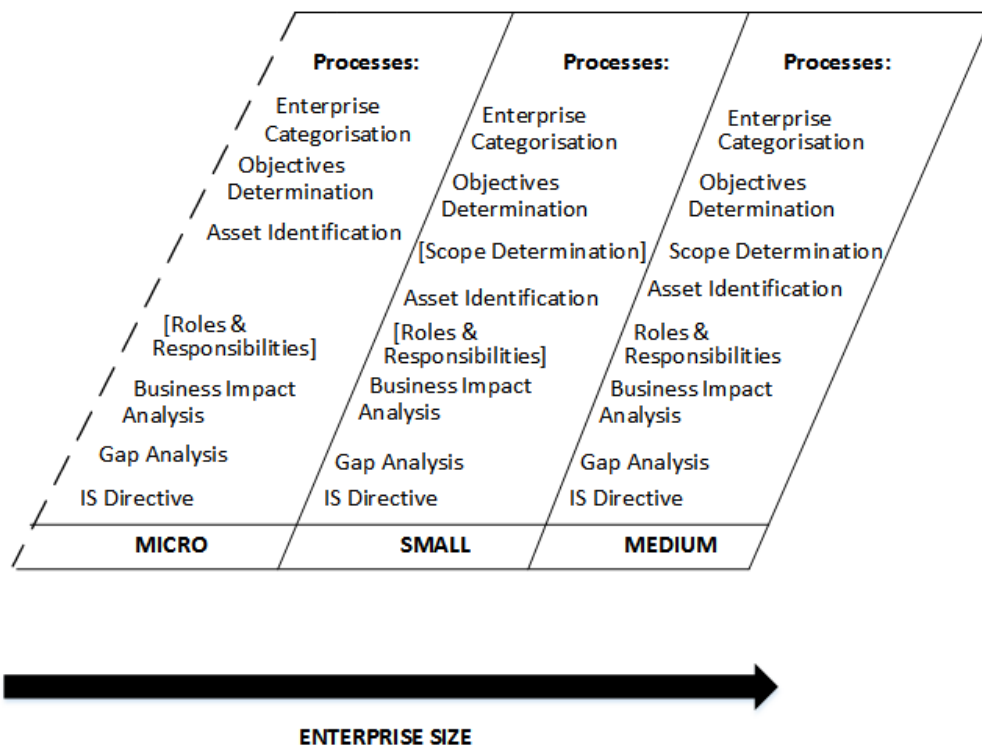


Figure 7.5: The Processes Aspect of MAISRSS

This section will discuss each of the processes that are presented in MAISRSS, as seen above. Furthermore, the researcher will discuss which category of SMME a process appears in and why this process is applicable to that category of SMME.



### 7.6.1 Enterprise Categorisation

This section discusses the Enterprise Categorisation process. This process is applicable to micro, small and medium enterprises. As seen in the discussion above, the scope of an ISMS is relative to the size of an SMME. According to the National Small Business Act (NSBA) of 1996, SMMEs are categorised, according to a number of characteristics. These characteristics include the number of full-time paid employees of the enterprise, the total gross assets of the enterprise, as well as the annual revenue generated by the SMME. Therefore, these characteristics are often referred as criteria to determine the size or category of the SMME. A list of the characteristics of SA SMMEs, according to the NSBA (The President's Office, 1996), can be found in Table 4.1 in section 4.6 of Chapter 4.

As seen in section 4.3 of Chapter 4, three major categories of SMMEs exist in SA. These categories are: micro, small and medium enterprises. Therefore, the process aspect of the MAISRSS categorises SMMEs into one of the three categories of SMMEs. An SMME can then perform only the processes applicable to that category of enterprise. Thus, all enterprises should use the criteria of the NSBA, or other guiding SA legislation to determine in which category of SA SMMEs the enterprise belongs.

According to the processes of MAISRSS, following an enterprise categorisation, the objectives of the organisation should be determined. Thus, the next section of this chapter, will discuss the process in which SMMEs determine their unique objectives.

### 7.6.2 Objectives Determination

The section below discusses the Objectives Determination process. The purpose of this process for SMMEs to determine their business and information security objectives. An objective is defined as an aim or intention (Oxford University Press, 2007, p. 398). Thus, it may be concluded that information security objectives define the aim or intention of an enterprise relative to information security. As discussed in section 3.2 of Chapter 3, one of the three sources of information security requirements comprises the principles, objectives and business requirements of an enterprise for information processing. Determining the business and information security objectives of an enterprise is important; as it also has an impact on the industry-specific legislation with which an enterprise must comply.

An example of industry-specific legislation in the SA medical professionals context is the Health Professions Act 56 of 1974. The purpose of this Act is to provide control over the education, as well as the training and the registration of practising health professionals registered under the Health Professions Council of South Africa (HPCSA) and related boards. Therefore, all enterprises registered with the HPCSA would be required to comply with the Health Professions Act.

In determining their business and information security objectives, SMMEs should also establish the vision of the enterprise pertaining to its business operations and information security. In simpler terms, SMMEs should determine what the purpose for the existence of the enterprise is.

An example of a business objective related to the early example, is that the SMME could have the intention to offer services related to the registration of health professionals in SA. Therefore, this SMME would be obliged to comply with the regulations of the Health Professions Act 56 of 1974. An intention to reduce the success of attacks on the integrity of confidential information by 20 per cent within a specified period is an example of a simple information security objective.

Thus, to accurately determine the information security requirements of an SMME, MAISRSS suggests that SMMEs should determine their business and the

information security objectives. Through the unique business and information security objectives, industry-specific legislation applicable to the enterprise can also be determined. Knowing the industry-specific legislation is vital; as it is also one of the sources of information security requirements, as seen in section 3.2 of Chapter 3.

After an SMME has determined its business and information security objectives, the SMME should identify the information assets that are critical to its business objectives. The process of asset identification is discussed in the next section of this chapter.

### 7.6.3 Asset Identification

This section discusses the Asset Identification process. The Asset Identification process is applicable only to small and medium enterprises.

As seen in the previous section, the Objectives Determination process concluded with SMMEs having determined their business and information security objectives. Furthermore, section 7.6.2 concluded that once an enterprise has determined its business objectives, it should identify the information assets that are critical to achieving those business objectives. Thus, this section will describe the Asset Identification process, in which SMMEs are guided in identifying their information assets.

Information assets were defined in section 2.4.1 of Chapter 2 as data of useful meaning to an organisation. The definition also includes any processes and systems that involve the creation, processing, transmission or storage of such data (DTI, 2004, p. 3; Brotby, 2009, p. 7). An information asset can range from customer lists and financial information to medical records, research findings and business proposals, to name just a few (Tipton & Krause, 2006, p. 5; Brotby, 2009, p. 7).

Similar to the ISO/IEC27003 (2010, p. 23), the MAISRSS suggests that in identifying its information assets, an enterprise should identify and list the following in an information asset inventory:

- (a) The unique name of the process or information asset;
- (b) A description of the process or information asset and its associated state (created, stored, transmitted or deleted);
- (c) The criticality of the process or of the information asset, to the enterprise (critical, important or merely supporting);
- (d) Who is responsible for the information asset or process, such as an organisational unit (discussed further in section 7.6.5.; roles and responsibilities);
- (e) Any processes that require input from this process or information asset or output to it;
- (f) ICT applications which support the process or the information asset;
- (g) Classification of the information asset, such as how long the information asset may be stored and which of its critical characteristics (confidentiality, integrity, availability, etc.) are most the important.

The process of Asset Identification, as seen above is intended to guide SMMEs in identifying their information assets and building an information asset inventory. However, this list is inclusive of all of the information assets of an enterprise. Therefore, the process discussed in the next section of this chapter describes demarcating the scope of information assets to include in the information security governance process within an enterprise.

#### **7.6.4 Scope Determination**

The following section is a discussion of the Scope Determination process. This process is applicable only to medium enterprises. According to Calder (2009, p. 57), the smallest of enterprise should include all information assets in the information security governance scope. While larger enterprises should determine which of their information assets are essential to include in the information security governance scope. Therefore, this section describes the scope determination process, in which

small and medium enterprises determine the scope of their information security governance.

“Simple situations require simple solutions” (Calder, 2009, p. 57). Thus, as mentioned above, the information security governance scope of micro enterprises should include everything within the enterprise that resembles an information asset and is involved with the processing, creation, storage, transmission or destruction of information assets. As seen in Figure 7.5, small enterprises have the option of either including everything in their information security governance scope, or performing a Scope Determination process. Optional processes are indicated by means of square brackets [ ].

Medium enterprises generally have more employees and a greater number of information assets than micro and small enterprises. Hence, it is important that medium enterprises perform a Scope Determination process to identify the information assets of the enterprise, which would be included in the information security governance scope. The information security governance scope is determined by identifying the applicability and the boundaries of the information security governance scope within the enterprise (ISO/IEC27001, 2013, p. 1).

Thus, in performing a Scope Determination process, enterprises would consider the criticality of the information asset, the business functions which depend on the information asset, as well as the classification of the information asset, the legal and regulatory requirements, and who is responsible for the information asset, as seen in the Asset Identification process. Thereby, an enterprise can determine whether or not an information asset falls within the boundaries of the information security governance scope.

The following process describes how the roles and the responsibilities for the protection of an information asset should be determined in SMMEs.

### 7.6.5 Roles and Responsibilities

The Roles and Responsibilities process. This process is about identifying information asset owners. The previous process, Scope Determination, described a process for SMMEs to determine the information assets that are essential to the business objectives of the enterprise. Furthermore, it was suggested that the essential information assets should be included in the information governance scope of the enterprise. The Scope Determination process therefore relies on input from the Asset Identification process, in which the information assets were labelled accordingly in an information asset inventory. One such label, included who is responsible for the protection of each information asset and its related systems and processes. Therefore, this section of the chapter, will described a process for assigning these responsibilities.

The Roles and Responsibilities process is all about identifying and appointing information asset owners. An information asset owner is an individual, or an organisational unit, who is given the responsibility of ensuring the protection of their assigned information asset. Such responsibilities require that the information asset owner should be aware of the state and the use of the information asset at all times (ISO/IEC27002, 2013, pp. 13-14).

Although ISO/IEC27002 (2013, p. 13) recommends that the information security committee should be the information asset owners within an organisation, it is evident that an information security committee often does not exist in most SMMEs. Furthermore, from the discussion in section 4.8 of Chapter 4, and the findings of the survey in Chapter 6, it was concluded that most SMMEs do not have the expertise or the resources to form an information security committee.

Therefore, it is convenient that an information asset owner could also be an individual or organisational unit within an enterprise. However, it is a requirement that the information asset owner be responsible for the creation, development, use and protection of the information asset and its related processes and systems (ISO/IEC27005, 2011, p. 4). Thus, it is recommended that the role of information

asset owner be assigned to an individual within an enterprise or organisational unit, who is also responsible for delegating tasks and the handling of information assets (ISO/IEC27003, 2010, p. 52).

Thus, the MAISRSS recommends that SMMEs appoint individuals, such as managers, in the role of information asset owner. In micro and small enterprises, a single manager might oversee all tasks and handling of information assets, making him/her the information asset owner for the entire enterprise. However, the manager can still delegate specific tasks or responsibilities to individuals within the enterprise; thereby, making this process optional for micro and small enterprises.

Medium enterprises often have a larger workforce than micro and small enterprises, as seen in Table 4.1 of Chapter 4. Therefore, more individuals often oversee the various organisational units. Thus, performing the Roles and Responsibilities process is mandatory for medium enterprises.

As information asset owners are responsible for the creation, protection and use of information assets. Therefore, they should be aware of the impact that a potential information security breach can have on the information asset, for which they are responsible and ultimately, on the enterprise. Thus, information asset owners should be involved in the Business Impact Analysis process, as can be seen in the following section.

### **7.6.6 Business Impact Analysis**

The section below discusses the Business Impact Analysis process. It is recommended that all categories of enterprises perform this process. It was mentioned in the previous section that information asset owners should be involved in determining the impact that a potential information security breach could have on the enterprise. This section of the chapter will describe the process of the MAISRSS, in which SMMEs assess the impact of a potential information security breach. The Business Impact Analysis process of the MAISRSS is based on the identification of consequences from ISO/IEC27005 (2011, p. 16).

The impact of a potential successful information security breach can include a loss of effectiveness, a loss of business reputation, legal matters, or other damage to an enterprise. Thus, enterprises should conduct a Business Impact Analysis on all of the information assets within the information security scope (ISO/IEC27005, 2011, p. 16). Information assets within the information asset inventory can be assessed individually or categorised (ISO/IEC27003, 2010, p. 52). According to the MAISRSS, SMMs can categorise, information assets according to any of the details about the information asset, listed in the information asset inventory. A few of these details are seen in section 7.6.3 of this chapter; and they are listed below:

- The processes and systems related to the information asset;
- The criticality of the information asset to the business objectives;
- Who the information asset owner is;
- The state of the information asset (stored, deleted, transmitted or created);
- The classification of the information asset (e.g. personally identifiable information, medical records, etc.); or
- According to the critical characteristics which are the most important facts about the information asset (e.g. confidentiality, integrity, etc).

The impact of a potential information security breach can be rated as very high, high, medium, low or negligible to list just a few options. When considering the impact of a potential information security breach, information asset owners should consider the following factors, as listed in the ISO/IEC27005 (2011, p. 16):

- Investigation and repair time;
- Work time lost;
- Opportunity lost;
- Costs to repair the damage; and



- The impact on the reputation of the enterprise.

When an enterprise has successfully analysed the impact that a potentially successful information security breach could have on its business operations; the enterprise must determine whether adequate information security is in place to reduce the success of information security breaches. Thus, a process to assess the current state of information security in the enterprise is described in the next section of this chapter.

### 7.6.7 Gap Analysis

The Gap Analysis process will be discussed in this process. This process is also applicable to all three categories of SMMEs. An information security assessment is an assessment of the current state of information security within an organisation, in comparison with the information security objectives of the enterprise (ISO/IEC27003, 2010, p. 24). Simply stated, an SMME would conduct an information security assessment to identify where the gap exists in the information security of the enterprise.

Furthermore, a gap analysis identifies the gap between the requirements of a standard or those of legislation and the current state of information security within an enterprise (Calder, 2009, p. 49). The identification of existing information security controls and the assessment of the current state of information security within an enterprise, should be done to avoid the unnecessary cost and the work of duplicating already existing information security controls and over protecting information assets (ISO/IEC27005, 2011, p. 15).

Figure 7.6, below, is a graphical representation of the objective of a gap analysis.

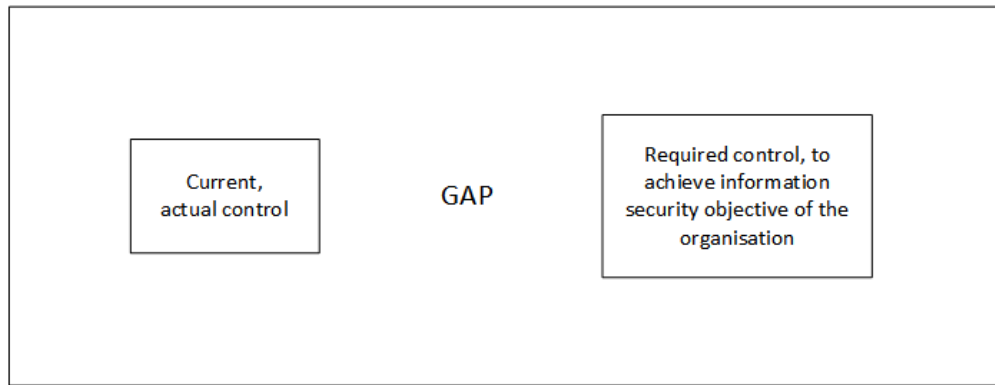


Figure 7.6: A graphical depiction of Information Security Gap Analysis. Adapted from Calder (2009, pg 61).

A number of methods for conducting an information security gap analysis have been reported in the literature. Some of these methods refer to an information security risk analysis type of process (ISO/IEC27005, 2011, p. 15). Other methods refer to an information security assessment (ISO/IEC27002, 2013, p. 24); while yet another method refers to a gap analysis as part of an information security risk assessment (Calder, 2009, p. 49).

Concerning the information security risk analysis process, ISO/IEC27005 (2011, p. 15), indicates that the current state of information security and the information security controls of an enterprise should be identified and assessed, as explained below:

- Documents relating to current information security controls within the enterprise, must be reviewed. These documents should contain information about the state of the implementation plan and the existing information security measures;
- Individuals responsible for information security must be consulted, wherever such individuals are available. Information asset owners and the users of information assets should also be consulted about their use, or the manner of implementation of information assets and the information security measures.

- To perform an information security assessment, an on-site review of the physical information security controls should be conducted. Such an on-site review would entail comparing the list of implemented information security measures, with the list of information security measures that should already be there. Furthermore, the effectiveness of the existing information security measures and whether or not they are functioning correctly should also be reviewed; and
- Finally, the results of an information security audit should also be reviewed.

The information security assessment referred to in ISO/IEC27003 (2010, p. 24), describes the following approach for assessing the current state of information security and information security measures within an enterprise:

- The information assets concerning information security requirements should be selected;
- To create a comprehensive flow chart covering the main information assets of the enterprise, including the infrastructure, if one is not already in existence;
- Discuss with suitable key personnel and analyse what the current state of information security is within the enterprise, in comparison with the information security objectives of the enterprise;
- Determine the information security measure deficiencies by comparing current information security measures with the previously identified information security measure requirements; and
- The assessment of the current state of information security within the enterprise should be completed and documented.

Additionally, Calder (2009, p. 50), refers to various tools, such as vulnerability assessment tools, penetration testing and information security risk assessment tools to measure the gap in the state of information security within the enterprise. The MAISRSS, does not prescribe or recommend any specific method for conducting an

information security gap analysis. However, it is recommended that all categories of SMMEs should conduct an information security gap analysis.

Typically, the output of the Information Security Gap Analysis process would be a document containing details of the current state of information security within the enterprise and how it compares with the information security objectives of the enterprise.

Although, Calder (2009, p. 49), claims that conducting an information security gap analysis is not a useful process in the creation of an ISO/IEC27001 compliant ISMS, the goal of MAISRSS is not to create an ISO/IEC27001 compliant ISMS, but to propose a simplified method for SMMEs to establish their information security requirements. SA SMMEs can then use these information security requirements that should be aligned with the business and information security objectives of the enterprise, in order to build an ISMS that suits the unique information security requirements of the enterprise. As such, MAISRSS recommends that all categories of SMMEs using MAISRSS, should conduct an information security gap analysis.

### **7.6.8 Information Security Directive**

This section discusses the final process of the process aspect. This process is applicable to all categories of SMMEs. The outcomes of the previously discussed processes each form a component of the sources of an information security requirement. Thus, it may be concluded that the information security requirements of an enterprise, which completed all of the previous processes, have been established.

Having established their unique information security requirements, SMME CEO-owner managers set out the approach of the enterprise to manage its information security requirements and to attain the information security objectives. Therefore, ISO/IEC27002 (2013, p. 2) recommends that the strategic-level management of an enterprise should define an information security policy. In general, a policy contains a statement of the overall intention and direction of the enterprise, as formally expressed by the management of the enterprise. The strategic-level man-

agement of the enterprise guides all the actions and the decisions concerning the topic of the policy. The policy can then be seen as the issuing of organisational directives related to the topic of concern (ISO/IEC27003, 2010, p. 57).

However, as the MAISRSS only communicates the information security requirements of the enterprise, it is not considered as an information security policy. Rather, the output of the MAISRSS information security (IS) directive process, is an information security directive itself.

According to ISO/IEC27002 (2013, p. 2), the information security policy of an enterprise should address:

- (a) Business strategy;
- (b) Regulatory, legislation and contracts; and
- (c) The current and projected information security threat environment.

Thus, the information security directive of an SMME should contain statements concerning:

- (a) A definition of the information security objectives and principles to guide all activities pertaining to information security. This was addressed in the Objectives Determination and the Scope Determination processes;
- (b) The assignment of general and specific responsibilities for the protection of information security assets. Hence, the identification of information assets and the appointment of information asset owners in the Asset Identification and the Roles and Responsibilities processes, respectively; and
- (c) The procedure for handling any deviations and exceptions from the normal. The Business Impact Analysis and the Gap Analysis processes determined the impact of potential information security breaches and the required information security levels, respectively. Thus, the required information security is identified. Therefore, SMMEs can also plan how to handle

any exceptions and deviations, based on the selected information security measures.

Additionally, the information security directive developed through the MAISRSS can have the following items, as adapted from ISO/IEC27003 (2010, p. 58):

1. **Introduction-** This is a brief explanation of the topic of the directive, as well as a short overview of what is to be covered in the directive;
2. **Scope-** Where the scope identification outcomes is explained and what is to be addressed by the directive, including why some information assets are excluded from the information security scope;
3. **Related Policies-** Describing other policies relevant to the fulfilment of the information security requirements and the information security objectives of the organisation. These include issue specific policies, such as those about the selection of information security controls.

The following section of this chapter provides a brief summary of the discussions of Part I of Chapter 7.

## 7.7 Summary

As seen in section 7.1 of this chapter, the chapter comprises two parts, Part I and Part II. This section of Part I recounts the discussions in Part I of Chapter 7.

Part I of this chapter consisted largely of a discussion of the MAISRSS, which is the model developed through this research study. The development of the MAISRSS was guided by the seven draft principles, as discussed in section 7.2 of this chapter. As seen in section 7.3 of this chapter, it was concluded that the MAISRSS best fits the definition of a model rather than that of a framework. Thus the MAISRSS was declared to be a model and not a framework.

In a section titled: “Constructing the MAISRSS” (section 7.4), the procedure followed in constructing the model was described. The procedure included the development of a theoretical model, which was deemed as not being representative of the typical corporate governance structure of most SMMEs. Thus, as seen in section 7.5, the flat CEO-centric corporate governance structure of the MAISRSS was discussed. Furthermore, the process aspect of the MAISRSS was discussed in section 7.6. The processes aspect describes the processes that need to be followed for SA SMMEs to determine their unique information security requirements. Additionally, an information security directive is produced explaining the organisational strategy to meet the information security requirements of the enterprise.

Part II of Chapter 7, will discuss an automated tool that was developed to automate the manner in which SMMEs determine their information security requirements. The automated tool was developed, based on the processes of the MAISRSS.

**The Automated Tool for the  
Alignment of Information  
Security Requirements within SA  
SMMEs**



## 7.8 PART II: Defining the Automated Tool

As mentioned in section 5.7.2, of Chapter 5, a proof-of-concept prototype was constructed. The prototype was in the form of an automated tool developed in Microsoft Excel by using the Visual Basic for Applications (VBA) language. According to Olivier (2009, p. 52), a proof of concept prototype demonstrates that a proposed concept, such as a new model, actually works in practice. Thus, this part of Chapter 7, will demonstrate how a simple Microsoft Excel tool was developed to automate the processes of the MAISRSS.

Therefore, Part II of Chapter 7 is divided into similar sections, as the discussion of the processes aspect discussion in Part I of this chapter. In each section of Part II of this chapter, screen shots will be used to demonstrate the layout of the automated tool. While a discussion will describe the purpose of each process of the automated tool. The first process of the automated tool is enterprise categorisation.

## 7.9 Automated Enterprise Categorisation

The automated enterprise categorisation, is the first process of the automated tool. Similar to the Enterprise Categorisation process of the MAISRSS, the automated enterprise categorisation attempts to categorise SMMEs as either a micro, small or medium enterprise. Therefore, the criteria from the NSBA (The President's Office, 1996) was used to categorise the enterprises in the Enterprise Categorisation process of the automated tool. Three questions (**a** in Figure 7.7) are used to determine the extent to which an enterprise satisfies the criteria for a specific category of SMME. Enterprises are required to indicate their annual revenue in rands; the number of full-time paid employees and the value of the total gross assets of the enterprise (in rands).

As seen in Figure 7.7 below, radio button controls (**b** in Figure 7.7) were used to ensure that users selected only one option as an answer to each question.

Enterprise Categorisation		Score
The aim of this process is to categorise the enterprise according to criteria of the National Small Business Act of 1996		
a	1. How many full-time paid employees does your enterprise currently employ?	
	<input type="radio"/> Between 1 and 5	0
	<input type="radio"/> Between 6 and 50	1
	<input checked="" type="radio"/> Between 51 and 200	2
	b	
	2. How much does your enterprise make in annual revenue?	
	<input type="radio"/> Between R0 and R150 thousand	0
	<input type="radio"/> Between R151 thousand and R 25 million	1
	<input checked="" type="radio"/> Between R25.1 million and R 50 million	2
	c	
3. How much in total gross assets is your enterprise currently worth?		
<input type="radio"/> Between R0 and R 100 thousand	0	
<input checked="" type="radio"/> Between R101 thousand and R 4.5 million	1	
<input type="radio"/> Between R 4.6 million and R 18 million	2	

Figure 7.7: The automated enterprise categorisation process

A value assigned to each radio button answer option is used to accumulate a score for the enterprise categorisation process (c in Figure 7.7). For example, a selection of the option “Between 6 and 50” for the number of employees, adds a value of one to the cumulative score. A range is then used to categorise the SMME according to the cumulative score. A cumulative score of between five and six, will be categorised as a medium enterprise. The points for each answer set and the cumulative score are hidden from the user in each of the automated processes.

Similar to the enterprise categorisation process in the MAISRSS, all the categories of SMMEs should perform the enterprise categorisation process. The user can then click the ‘Next’ button to proceed to the automated objectives determination process.

## 7.10 Automated Objectives Determination

As seen in Part I of this chapter, the objectives determination process has the purpose of determining the business and information security objectives of an enterprise (see section 7.6.2). The automated objectives determination process exists for the same purpose. However, the automated objectives determination process simplifies the determination of the information security objectives of an enterprise.

Users of the automated tool are only required to answer five questions pertaining to their enterprise (see label **a** in Figure 7.8). The first question (label **b** in Figure 7.8) requires that the user specifies three business objectives, which are related to the vision and mission of the enterprise. To simplify the determination of information security objectives, users are required to select answers to questions, according to the priorities of the enterprise. Users are restricted to selecting a single answer for each question, by using the radio button controls (see label **c** in Figure 7.8).

The automated objectives determination process attempts to determine the order of importance in which the enterprise prioritises the following information security objectives:

- Business continuity and disaster recovery;
- Resilience to information security incidents;
- Addressing legal, contractual and compliance obligations; and
- Protecting the strategic information assets of value to the enterprise.

Information Security Objectives Determination		Score
The objective of this process is to determine the business and information security objectives of the enterprise.		
<b>Business Objectives</b>		
1. List three business objectives related to the mission of the enterprise.		
<b>Information Security Objectives</b>		
2. <input checked="" type="checkbox"/> In the event that an information security incident occurs, how important is facilitating business continuity and disaster recovery?		
<input type="checkbox"/>	Extremely important	3
<input type="checkbox"/>	Considerably important	2
<input type="checkbox"/>	Important	1
<input type="checkbox"/>	Not applicable	0
3. How important is it for the enterprise to improve resilience to information security incidents?		
<input type="checkbox"/>	Extremely important	3
<input type="checkbox"/>	Considerably important	2
<input type="checkbox"/>	Important	1
<input type="checkbox"/>	Not applicable	0
4. How important is addressing legal/contractual compliance/liabilities to the enterprise?		
<input type="checkbox"/>	Extremely important	3
<input type="checkbox"/>	Considerably important	2
<input type="checkbox"/>	Important	1
<input type="checkbox"/>	Not applicable	0
5. How important is the protection of assets of strategic value to the enterprise?		
<input type="checkbox"/>	Extremely important	3
<input type="checkbox"/>	Considerably important	2
<input type="checkbox"/>	Important	1
<input type="checkbox"/>	Not applicable	0

Figure 7.8: The automated objectives determination process

As marked as label **d**, values from 0 (not important at all) to 3 (extremely important), are provided as options to questions 2 through 5. Although the score is not shown to the user, variables are used to store the value assigned to the selected option for each question. The value stored in each of the four variables, is automatically compared, in order to determine the order of importance of the four information security objectives mentioned earlier in this section. A higher score, means that an item features higher on the list. According to the MAISRSS, the process which follows an objectives determination, is the asset identification process. Therefore, the next process of the automate tool is the automated asset identification process.

## 7.11 Automated Asset Identification

The Asset Identification process attempts to build an information asset inventory as seen in section 7.6.3. Therefore, in the automated Asset Identification process,

the users are required to answer questions about the information assets of the enterprise.

Unlike the seven fields of the information asset inventory as seen in section 7.6.3 of Part I, the automated asset identification only requires input for six fields. Due to space constraints, the users are not required to provide a description for information assets in the automated Asset Identification process (refer to Figure 7.9):

- The name or asset number of the information asset (label **a**);
- How critical the information asset is to the business operations of the enterprise (critical, important or supporting) (label **b**);
- The state of the information asset (created, deleted or stored) (label **c**);
- How long the enterprise is allowed to store the information asset (label **d**);
- The date of creation or purchase on an information asset (label **e**); and
- Finally, which of the characteristics is most significant to the enterprise (confidentiality, integrity, availability, business continuity or non-repudiation) (label **f**).

A combination of drop-down lists, check-box selections and text-input controls are used to gather the data from users. The interface of the automated Asset Identification process is seen in Figure 7.9.

Asset Identification						
Name/asset # of information asset	Criticality	State	Storage duration	Date of creation	Significant characteristics	Key/Legend
Financial statements of partner	Important	Deleted	5 hours	25-05-2018	<input type="checkbox"/> C <input checked="" type="checkbox"/> I <input type="checkbox"/> A	C- Confidentiality
Unpatented design of locomotive	Critical	Created	3 Years	22-02-2017	<input checked="" type="checkbox"/> C <input checked="" type="checkbox"/> I <input checked="" type="checkbox"/> A	I- Integrity
3					<input type="checkbox"/> C <input type="checkbox"/> I <input type="checkbox"/> A	A- Availability

Figure 7.9: The automated asset identification process

Whenever a user selects a significant characteristic (I= integrity, C= confidentiality and A= availability), the appropriate counter is incremented. Individual counters are used for each significant characteristic; and they are an indication of the number of information assets with that significant characteristic. Information assets can have more than one significant characteristic; therefore, users are able to select more than one significant characteristic per information asset. The findings of the automated Asset Identification process, such as the criticality and the significant characteristics, are used to group information assets into various categories in one of the later processes of the automated tool.

The automated Asset Identification process, like the Asset Identification process of the MAISRSS, is the last process which is mandatory for all categories of SMMEs (see section 7.6). Following the automated Asset Identification process, enterprises should determine which information assets to include in the information security governance scope, as seen in section 7.6 of Part I. It was also mentioned in section 7.6.4 that the smallest enterprises should include everything in the ISMS scope. Therefore, micro enterprises do not perform the Scope Determination process. Small enterprises have the option of performing the automated Scope Determination process or proceeding to another optional process (roles and responsibilities). A message box control used to present the various options to the users. Medium enterprises are automatically directed to the automated Scope Determination process. The automated Scope Determination process is discussed in the next section of this chapter.

## **7.12 Automated Scope Determination**

As seen in the previous automated process (automated Asset Identification), enterprises should build an asset inventory of all the information assets within the enterprise. The asset inventory allows enterprises easier protection of the information assets, as they appear on a single comprehensive list. However, some information assets may belong to a third party service provider; and therefore, fall outside the boundaries of protection of the enterprise. Therefore, SMMEs should demar-

cate the boundary of their information security governance by specifying which information assets are included in the scope of information security governance (see Part I section 7.6.4).

Information assets from the asset inventory, with a state of either stored or created, automatically populates the automated Scope Determination. An information asset with the deleted state is exclusively allowed in this instance for illustrations (see the state of the first information asset in Figure 7.9). A number of fields, such as criticality, state, storage duration and significant characteristics of the information asset also automatically populate the automated Scope Determination.

Fields such as the BIA (business impact analysis) Applicability (**b**), Belongs to SP (service provider) (**c**), Include in ISMS scope (**d**) are added to the interface in this process (see Figure 7.10). Label **a**, represents the information assets, and was already mentioned in the automated Asset Identification process. The BIA Applicability field displays the counter for the relevant significant characteristics. If an information asset is labelled as having the significant characteristics I (integrity) and C (confidentiality), but not A (availability), the overall counters for I and C will show the number of information assets with that characteristic; while the counter for A will display a zero.

An information asset belonging to a service provider (SP), is automatically excluded from the information security governance scope. The responsibility for protecting the information asset is transferred to the third party service provider. The field Include in ISMS scope, allows users to include or exclude information assets from the scope of information security governance. As seen in Figure 7.10, label (**d**), information assets indicated with a state of deleted, and those that belong to third party SPs cannot be included in the ISMS scope. All information assets indicated as being critical to the enterprise cannot be excluded from the scope of the ISMS.

**Scope Determination**  
The objective of this process is to determine the information assets to include in the scope of the ISMS.

Information asset name	Criticality	State	Storage duration	Date of creation	Significant characteristics	BIA Applicability	Belongs to SP?	Include in ISMS Scope
Financial statements of partner	Important	Deleted	5 hours	25-05-2016	I	C=0 I=3 A=0	Yes	No
Unpatented design of locomotive	Critical	Created	3 years	22-02-2017	C, I, A	C=2 I=3 A=1	No	Yes
TR1#S2100 Engine Design Specs	Important	Stored	15 years	30-09-2008	LA	C=0 I=3 A=1	No	Yes

**a** {

↑            ↑            ↑  
**b**            **c**            **d**

Figure 7.10: The automated scope determination process

Small enterprises, which performed the automated Scope Determination process are then given the option to proceed to the automated Roles and Responsibilities process, or directly to the automated Business Impact Analysis process. Contrary to this, medium enterprises are automatically directed to the automated roles and responsibilities process, according to the MAISRSS (as seen in section 7.6). The next section discusses the automated Roles and Responsibilities process.

### 7.13 Automated Roles and Responsibilities

It was reported that an asset owner should be assigned to each information asset within the scope of the ISMS. The responsibility of an asset owner in this context, is to ensure the protection of each information asset for which they are responsible.

Therefore, as labelled **(a)** in Figure 7.11, only those information assets within the scope of the ISMS are automatically imported to the automated roles and responsibilities process. In the smallest category of SMMEs, all information assets from the asset inventory are automatically imported to the automated roles and responsibilities process.

The user is also required to assign the information asset to the business unit or process in which it is primarily used (see label **b** in Figure 7.11). Each information asset is assigned an asset owner, as marked by label **(c)** in Figure 7.11. The date on which the information asset is assigned to an asset owner is also recorded (see label **d** in Figure 7.11).



Roles and responsibilities			
The objective of this process is to assign the responsibility of asset owner for each information asset within the ISMS scope.			
Name/asset # of information asset	Business Unit/Process	Assigned Asset Owner	Date of Assignment
Unpatented design of locomotive	Manufacturing	Thabo Ngonyane (manager )	2018-01-02
TRT#52100 Engine Design Specs	Manufacturing	Thabo Ngonyane (manager )	2010-05-03

a {

↑                      ↑                      ↑  
 b                      c                      d

Figure 7.11: The automated roles and responsibilities process

As discussed in section 7.6.5 in Part I of this chapter, micro and small enterprises commonly have fewer organisational units, if any. Therefore, the automated Roles and Responsibilities process is optional to these two categories of SMMEs. However, medium enterprises are larger with more employees and more organisational units and they should therefore perform the automated Roles and Responsibilities process.

In the next section of this chapter, the researcher will discuss the automated process in which asset owners analyse the potential impact of information security breaches on the enterprise.

## 7.14 Automated Business Impact Analysis

A loss of the significant characteristics of an information asset can have a negative impact on an enterprise, as reported in section 7.6.6 of Part I of this chapter. Thus, the automated Business Impact Analysis process attempts to automate the manner in which SMMEs establish the potential impact that the loss of a significant characteristic could have on the enterprise.

Therefore, the questions used to gather the data from users in the automated Business Impact Analysis process are categorised into: confidentiality, availability and integrity as demarcated by label **a** in Figure 7.12 (the three significant characteristics, as seen in section 7.11). The same answer sets are used for each of

the three questions in this automated process. Users of the automated process are allowed to select multiple answers to each of the questions (see label **b** in Figure 7.12). Each answer selection adds a value of one to the cumulative score of the category (label **c** in Figure 7.12).

The cumulative score of each category is used to analyse the magnitude of a potential loss of that specific significant characteristic of an information asset. Additionally, the category with the highest cumulative score indicates that a loss of that specific significant characteristic would have the greatest impact on the enterprise.

Figure 7.12 below, is a snapshot of the automated Business Impact Analysis process interface. Only the questions and answer sets for two categories (confidentiality and availability) are shown; and they are marked as label **(a)**.

Business Impact Analysis		Score
The objective of this process is to determine the impact that a potentially successful information security attack could have on the enterprise.		
<b>Loss of Confidentiality</b>		
1. What would be the result of the unauthorised disclosure of information or processes used by the enterprise?		
<input type="checkbox"/> Loss of customer confidence		1
<input type="checkbox"/> Damage to reputation (enterprise and/or clients and employees)		1
<input type="checkbox"/> Disruption in third parties transacting with the enterprise		1
<input type="checkbox"/> Infringement of laws / regulations		1
<input type="checkbox"/> Danger to personnel / user safety		1
<input type="checkbox"/> Attack on users' private life		1
<input type="checkbox"/> Loss of customers, loss of suppliers		1
<input checked="" type="checkbox"/> Loss of a competitive advantage		1
<b>Loss of Availability</b>		
2. What would be the result of authorised users not being able to access information and processes used for the operations of the enterprise?		
<input type="checkbox"/> Loss of customer confidence		1
<input type="checkbox"/> Damage to reputation (enterprise and/or clients and employees)		1
<input type="checkbox"/> Disruption in third parties transacting with the enterprise		1
<input type="checkbox"/> Infringement of laws / regulations		1
<input type="checkbox"/> Loss of customers, loss of suppliers		1
<input type="checkbox"/> Loss of a competitive advantage		1
<input type="checkbox"/> Financial losses		1
<input type="checkbox"/> Breach of contract		1
<input type="checkbox"/> Disruption of a third party's operation		1
<input type="checkbox"/> Inability to provide the service		1
<input type="checkbox"/> Material damage		1
<input type="checkbox"/> Inability to fulfill contractual obligations		1

Figure 7.12: The automated Business Impact Analysis process

Having established which of the significant characteristics could potentially have the greatest impact on the enterprise, asset owners must ensure that their information assets are adequately protected against information security breaches.

Therefore, asset owners should also participate in the automated Gap Analysis process, as will be discussed in the next section of this chapter.

## 7.15 Automated Gap Analysis

As mentioned at the end of the automated Business Impact Analysis process, information asset owners should determine whether the enterprise has adequately protected their information security assets. Thus, the automated Gap Analysis process uses questions to gather the data from users and to perform a calculated estimation of where the gap exists in the information security efforts of the enterprise. Therefore, the user is required to answer a series of questions about information security attacks on the information assets of the enterprise (see Figure 7.13 label **a**).

The questions of this automated process are categorised, according to the significant characteristics of an information asset. This categorisation allows the same questions to be asked about information security attacks on each of the three significant characteristics of an information asset. As seen in Figure 7.13, the first category of questions pertains to information security attacks on the confidentiality of the information assets.

**Gap Analysis**  
This process seeks to establish the effectiveness of implemented information security controls if any have been implemented

**Confidentiality**  
The questions in this section pertain to incidents of unauthorised access to confidential information assets of your enterprise or business unit.

Information security Incidents		Score
What is the percentage of information security attacks to gain access to sensitive or confidential information, that have been successful last financial year?		
<input type="radio"/> 0% - 20%	} b	0
<input type="radio"/> 21% - 40%		1
<input type="radio"/> 41% - 60%		2
<input type="radio"/> 61% - 80%		3
<input type="radio"/> 81% - 100%		4
What is the percentage of the successful information security attacks on confidential information, targeted critical information assets?		
<input type="radio"/> 0% - 20%		0
<input checked="" type="radio"/> 21% - 40%		1
<input type="radio"/> 41% - 60%		2
<input type="radio"/> 61% - 80%		3
<input type="radio"/> 81% - 100%		4

Figure 7.13 includes three labels: 'a' is a bracket on the left side of the Confidentiality section; 'b' is a bracket on the left side of the first question's radio button options; 'c' is a bracket on the right side of the Score column for the first question.

Figure 7.13: The automated gap analysis process

Label **b** marks the answer sets used for the first four questions. Percentages are used as a metric to measure the ranges of successful information security attacks, which could have occurred in the past financial year. Each range of percentages is linked to a numerical value, as marked by label **c**. The corresponding numerical value is stored in a variable linked to the question, whenever a user selects an answer from the list of possible selections.

The first four questions (of which only two are shown due to space constraints) of the automated gap analysis process, as seen in Figure 7.13, gather the data about the target and the perpetrator of information security attacks. Firstly, the user is asked about the percentage of information security attacks on a specific significant characteristic of an information asset. Secondly, the user is required to answer questions pertaining to the criticality of the information security attack target. The third and fourth questions attempt to establish the percentage of information security attacks committed by employees and those committed by external parties, respectively.

For readability purposes, the automated Gap Analysis process was separated into two parts. Part 1, is seen in Figure 7.13 above. While Part 2 of the automated Gap Analysis process is seen in Figure 7.14 below.

What is the percentage of the successful information security attacks on confidential information assets were committed by employees (intentional and unintentional)?		
<input type="radio"/> 0% - 20%		0
<input type="radio"/> 21% - 40%		1
<input type="radio"/> 41% - 60%		2
<input type="radio"/> 61% - 80%		3
<input type="radio"/> 81% - 100%		4
What is the percentage of the successful information security attacks on confidential information assets were committed by external parties?		
<input type="radio"/> 0% - 20%		0
<input type="radio"/> 21% - 40%		1
<input type="radio"/> 41% - 60%		2
<input type="radio"/> 61% - 80%		3
<input type="radio"/> 81% - 100%		4
d }	Which of the following categories of information security controls does your enterprise implement to protect information assets against attacks on the confidentiality of the information assets (select all that are applicable)?	
	<input type="checkbox"/> Policy and procedure	1
	<input type="checkbox"/> Hardware (e.g. firewall and IPS)	1
	<input type="checkbox"/> Software (e.g. antivirus, IDS, IP address blacklisting)	1
	<input type="checkbox"/> Security personnel (e.g. security officers)	1
e }		
<input type="checkbox"/> No information security controls have been implemented		0
		f }

Figure 7.14: The automated gap analysis process part 2

As marked by label **d** in Figure 7.14, the final question of each category, pertains to the information security controls implemented by an enterprise. Thus, the users are required to select any number of information security measures, which their enterprise already implements to protect its information assets. The list of possible information security controls is marked by label **e**. This list is as seen below:

- Policy and procedure;
- Hardware (e.g. Firewall and IPS);
- Software (e.g. Anti-virus, IDS and IP address-blacklisting);
- Security personnel; and
- No information security controls have been implemented.

Each answer selection adds a value of one to the cumulative score for that question, except for the option of “No information security controls have been implemented”. Where no information security controls have been implemented, a value of zero is stored in the cumulative score variable (see label **f** in Figure 7.14).

Through the automated Gap Analysis process, SMMEs can analyse the effectiveness of their current information security measures. Thus, allowing SMMEs to identify the gap that exists in their current implementation of information security measures. All categories of SMMEs are required to perform the automated Gap Analysis process, as a gap in the information security of an enterprise can exist, regardless of the category of SMME.

## 7.16 Automated Information Security Directive

Organisations are governed through directives, which are issued by the strategic level management. The directive is how the strategic-level management guide the use of organisational resources to achieve specific objectives within the organisation (see Chapter 2, section 2.2.1).

The automated Information Security Directive process, was adapted from the Information Security Directive process in the MAISRSS. All of the outcomes of the previous processes are collated to form an information security directive. The purpose of the information security directive is to issue guidance to asset owners, about the information security requirements of the enterprise.

Various components are included in the information security directive, as can be seen in Figure 7.15. The snapshot of the information security directive, as seen in this dissertation, is divided into four parts that will be discussed below. No logical groups exist, the snapshot was simply divided for readability purposes.

Marked as **a** (in Figure 7.15), the first part of the template contains placeholders for the name and logo of the enterprise. Secondly, label **b** (in Figure 7.15), marks the sections of the information security directive. These include some section headings found in a typical information security policy, such as the policy title, the responsible executive and for whom the policy is intended.



<b>III. Definitions</b>			
<b>Information security requirements</b> - a measure of the information security required to adequately protect the information assets of the enterprise and avoid liability for successful information security attacks.			
<b>Confidentiality</b> - only those authorised to see the information should be able to do so.			
<b>Availability</b> - the required information should be readily available to authorised users when it is needed.			
<b>Integrity</b> - only authorised users should be allowed to make changes in a manner authorised by the enterprise.			
<b>IV. Information Security Objectives</b>			
[enterprise name], endeavours to support the need for access to information assets in order to achieve the business objective of the Company. Therefore, the Company acknowledges that a loss of the significant characteristics of the information assets could result in a disruption to the business operations of the Company. Thus, the Company sets out to achieve the following information security objectives to protect the significant characteristics of the information assets:			
[a list of the information security objectives from the automated objectives determination process]			
<b>V. Responsibilities</b>			
In ensuring that the information of the Company is protected, asset owners have been assigned to each information asset as seen in the list below. Asset owners are responsible for ensuring the well being of all information assets assigned to them.			
<b>Name/asset # of information asset</b>	<b>Business Unit/Process</b>	<b>Assigned Asset Owner</b>	<b>Date of Assignment</b>

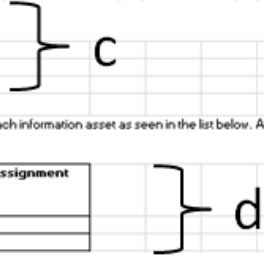


Figure 7.16: The Automated Information Security Directive Process (part 2)

The information security directive also includes a section tabling the assigned asset owners, and the information assets for which they are responsible. Any incidents regarding an information asset can thus be reported to the appropriate asset owner. Label **d**, in Figure 7.15, marks the information asset owner in the information asset assignment table in the information security directive.

The information security requirements of the enterprise are indicated by using a colour to fill the cells next to the appropriate significant characteristic of an information asset. Red means that the protection of that significant characteristic is not very ineffective; and it should be addressed immediately. Amber, means that the information security is moderate, but that it could be improved. While, green indicates that the information assets are currently adequately protected. See label **e** (in Figure 7.17), for an example of the information security requirements colour indicators. The colours in Figure 7.17 are used as an example only. None of the colours represent a specific significant characteristic of an information asset.



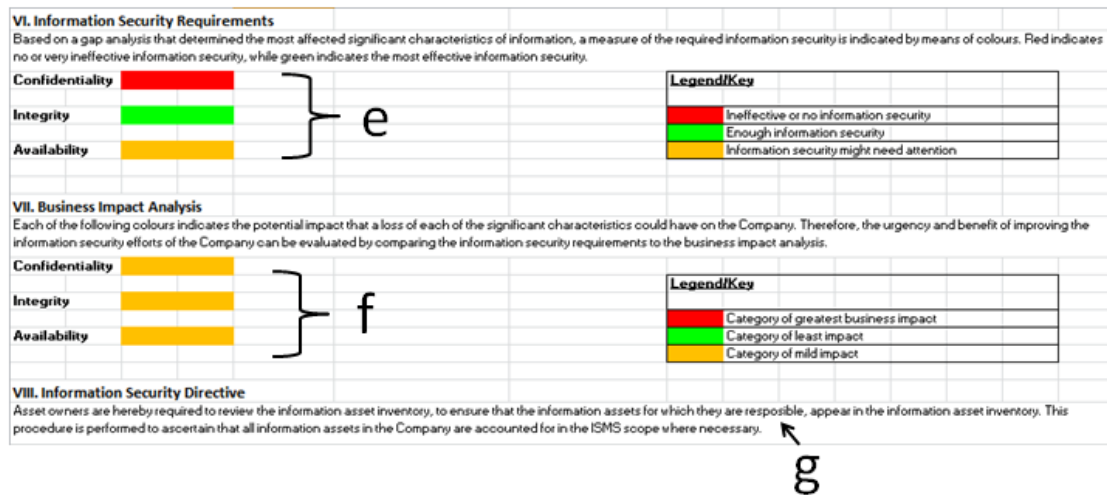


Figure 7.17: The Automated Information Security Directive Process (part 3)

It may also be of use for enterprises to know the potential impact of a successful information security breach. Thus, the findings of the automated business impact analysis are imported into the information security directive. Similar to the information security requirements, colours indicators are used to represent the magnitude of the potential impact of a successful information security breach. Red indicates the significant characteristic that would have the greatest impact on the enterprise if it were lost. As seen earlier, amber indicates that the impact would be moderate; while green indicates that the magnitude of the impact is of negligible size see label **f** (in Figure 7.17).

Enterprises can thus determine the benefit of addressing their information security requirements. As represented by label **f** in Figure 7.17, information asset owners would be able to see the potential impact of an information security breach. Once again, colours were used to represent the potential impact of a breach of the CIA of the information assets. Green indicates a low impact, amber indicates a considerable impact and red indicates a great impact. Thus it may be said that enterprises can see the potential impact that they can avoid by addressing their information security requirements. The information security directive marked (**g**), instructs asset owners to ensure that their information assets are within the scope

of information security governance; and that they are adequately protected from information security breaches.

Finally, asset owners are encouraged to perform searches on the internet to find further information about related policies and standards pertaining to the business objectives of the enterprise see label **h** (in Figure 7.18). In conclusion of the information security directive, a clause states that the information security directive should be reviewed at least once every financial year, or whenever there is a change in the configuration of the information asset inventory labelled **i** (in Figure 7.18).

<b>IX. Related Policies, Standards and Procedures</b>									
Related policies, standards and procedures provide further information on the liabilities and requirements for organisations. Such policies, standards and procedures can be found by searching for information security policies and standards related to the business objectives of the Company. The business objectives of the Company are listed below:									
<b>Business Objectives</b>									
[a list of business objectives from the objectives determination process]									
<b>X. Directive Review</b>									
This information security directive should be reviewed at the end of every financial year or if changes are made to the configuration of the information asset inventory.									

Figure 7.18: The Automated Information Security Directive Process (part 4)

When the information security directive, as discussed above, is completed, it can then be distributed to the appropriate parties. These include the various parties listed as the groups for whom this information security directive is intended.

## 7.17 Conclusion

It was stated in section 7.1 that the objectives of this chapter were to argue towards draft principles, and secondly to discuss the model developed from those draft principles. Subsequently, draft principles that guided the design and development of the model were derived, as seen in section 7.2. The researcher then described how these draft principles were used to design and develop the model, which is titled a ‘Model for the Alignment of Information Security Requirements within SA SMMEs’ (MAISRSS).

It was argued that the MAISRSS is a model and not a framework, according to the justification, as seen in section 7.3. Chapter 7 was then divided into two parts. Part I, included a discussion of the two aspects of the MAISRSS, namely the governance aspect and the process aspect. The governance aspect and the process aspect of the MAISRSS were each discussed in sections 7.5 and 7.6, respectively.

Part II of Chapter 7, was a discussion of the proof-of-concept prototype of the automated tool that was developed, based on the eight processes of the process aspect of the MAISRSS. The automated tool was developed to demonstrate the practical relevance of the MAISRSS and to automate the processes of the MAISRSS for SMMEs.

The following chapter (Chapter 8) of this dissertation will discuss the procedure followed in conducting expert interviews, which were used to evaluate the MAISRSS and the automated tool. The findings and the feedback from the evaluation will also be discussed in Chapter 8.

# Chapter 8

## Evaluating the MAISRSS and the Automated Tool

*“An error doesn’t become a mistake until you refuse to correct it.”*

-Orlando Battista

### 8.1 Introduction

In Part I of the previous chapter (Chapter 7), the MAISRSS, the proposed solution to the research problem stated in section 1.6.1 of Chapter 1, was introduced. Similarly, in Part II of Chapter 7, an automated tool, which was developed based on the MAISRSS, was introduced. As evaluation forms a crucial part of demonstrating scholarly work, this chapter intends *to provide an evaluation of both the proposed MAISRSS and the subsequent automated tool*. This is in line with the steps of the integrated research design, as discussed in section 5.6.3 of Chapter 5.

The discussion of the evaluation of the MAISRSS and the automated tool will begin by defining the approach that was used to evaluate both artefacts. Although expert interviews were defined in Chapter 5, this chapter provides a detailed definition. Following the definition of the evaluation approach, how the evaluation was conducted will be discussed in two separate parts that are identical in structure.

Part I of this chapter is a discussion of the evaluation of the MAISRSS; while, Part II of the chapter discusses the evaluation of the automated tool. Both Part I and Part II of Chapter 8, firstly report on the process of designing the evaluation instruments. Thereafter, the researcher discusses the feedback obtained during the evaluation process. In the light of this feedback, a discussion of how the artefact was adapted will follow. Finally, a number of concluding remarks will be drawn from each of the two parts of this chapter.

## 8.2 The Evaluation Approach

According to the integrated research design followed throughout this research study, any developed artefacts should undergo a process of evaluation. Through the evaluation, the extent to which the artefact is aligned with the draft principles derived in section 7.2 of Chapter 7, can be measured (Österle et al., 2010; Herrington et al., 2007). The evaluation of an artefact, against the provided elements, is a requirement of scholarly or academic work (Eco, 2015, pp. 27-30). Thus, the MAISRSS and the automated tool (the artefacts) were evaluated against the draft principles.

Owing to the academic freedom afforded through the inclusion of design-oriented IS research (Osterle et. al, 2010), the researcher was allowed to use various methods within the body of knowledge to evaluate the developed artefacts. As such, structured interviews were used to obtain feedback from the experts who evaluated the artefacts against the draft principles.

Kajornboon (2005) reports that structured interviews are interviews in which all the respondents are asked the same questions, with the same wording and in the same sequence. Therefore, Kajornboon (2005) claimed that structured interviews are a standardised form of interview. Due to constraints, such as geographical distance, the researcher resorted to electronic means of interviewing the experts, such as distributing the questionnaires via email. Thus, to ensure control over the sequence and the format of the obtained responses, structured interviews were

used.

The remainder of this chapter will discuss the evaluation of the MAISRSS and the automated tool in two parts, as mentioned in an earlier section.

# Evaluating the MAISRSS

## 8.3 PART I: Designing the Information Security Expert Interview

Due to the nature and purpose of the model, it was concluded that the involvement of an information security expert would be highly beneficial. Therefore, it was decided that the evaluation of the MAISRSS should be performed by an information security expert. Expert interviews and the characteristics of an expert were defined in section 5.7 of Chapter 5. These include the number of years of experience and the academic qualifications of the individual.

However, for this evaluation, academic qualifications were not considered. Instead, the researcher attempted to identify an information security expert as one who has had no less than five years of experience working in information security governance. Additionally, an individual performing duties pertaining to information security governance in SA SMMEs would be considered as being the ideal respondent for the expert interview.

Due to geographical distance and time constraints, electronic means were used to communicate with the experts for convenience. A suite of information on the research project and the MAISRSS was sent to an individual, identified as an information security expert based on the characteristics considered for this study (as mentioned above). The suite contained background information on the research study, a synopsis of the MAISRSS, a video describing the MAISRSS, and a questionnaire to be completed by the information security expert. The documents of the suite of information and the questionnaire are included in this dissertation as Appendix C. The video can be found on the compact disc accompanying this dissertation.

The purpose of the questionnaire was to provide a convenient, yet structured method to obtain the evaluation response of the information security expert. Therefore, the questionnaire formed the structured interview, consequently used as an expert interview in this research study. Structured interviews were defined in section 8.2 of this chapter. This part of the chapter will discuss the design,



as well as the data obtained from the information security expert interview. The discussion will take the form of a questionnaire similar to the one that was used to collect the data from the information security expert. Therefore, the structure of the discussion will be in three sections, namely: Background Information, General Principles and Draft Principles. Furthermore, a section will discuss the findings of the information security expert interview, and how these findings were used to refine the MAISRSS.

### **8.3.1 The Background Information**

Although academic qualifications were not considered, the respondents were given the option of stating their academic qualifications along with their name and surname. Thus, the Background Information section of the questionnaire primarily intended to establish the number of years of experience of the information security expert in the information security governance sphere. Furthermore, information security experts were asked to rank their confidence in answering those questions pertaining to information security governance, SA SMMEs, information security requirements and ISMS.

The information security experts were then asked several questions pertaining to the general principles on which this research study was based.

### **8.3.2 The General Principles**

The General Principles section of the questionnaire comprised six questions, which aimed to ascertain the extent to which the information security expert agreed with several of the premises. These premises formed the basis for the argument of this research study; and they are listed below:

- The importance of information security requirements;
- The importance of an ISMS;
- The complexity of some information security best practices and standards for SMMEs; and

- The flat corporate governance management structure of most SMMEs.

The extent to which the information security expert agreed with each of these premises was concluded to be an indication of how often the information security expert had encountered such; and it was not based necessarily on the validity of the actual premise.

The third and final section of the information security expert interview pertained to the draft principles which were derived in Chapter 7. In this section of the questionnaire, the information security expert was requested to evaluate the adherence of the MAISRSS to the seven draft principles.

### **8.3.3 The Draft Principles**

As mentioned in the previous section, the Draft Principles section was an evaluation of the extent to which the information security expert agrees that the MAISRSS adheres to each of the seven draft principles. Nine questions in total were used; and each was intended to establish the extent to which the MAISRSS adheres to a single draft principle.

Although the questions in this section do not explicitly ask about each draft principle, an association between the questions and the draft principles is assumed and can be easily identified.

## **8.4 Analysis and Results of the Information Security Expert Interview**

This section will discuss the results obtained from the information security expert interview and how it affects the MAISRSS. The responses obtained in each of the sections of the questionnaire, as presented earlier, will be discussed.

### 8.4.1 The Background Information

This section discusses the response of an information security expert in the Background Information section of the questionnaire. As mentioned earlier, providing the name, surname and highest academic qualification were optional. The respondent opted not to disclose this information.

Pertaining to their current occupation, the respondent indicated that their current occupation is IT Audit and Advisory. Further explaining that in their occupation, the respondent fulfils the role of Technology Advisory Manager in their organisation.

Responding to the extent to which their academic qualification is related to information security governance, the respondent indicated that their academic qualification is related to information security governance. Moreover, the respondent stated that they had at least five years of work experience in the information security and information security governance field. Consequently, the respondent agreed that they are confident in answering the questions pertaining to information security and information security governance.

Although the respondent reported that they are somewhat experienced in working with information security governance in SMMEs, they indicated that their work frequently involves information security and information security governance in SMMEs. Hence, the respondent indicated that they were confident in their knowledge and experience to answer questions pertaining to information security and information security governance in SA SMMEs. However, the respondent remained neutral about their confidence in answering questions about an ISMS. Similarly, the respondent was neutral about confidently responding to questions pertaining to information security requirements.

Based on the above, the researcher has ascertained that the respondent had the characteristics of an information security expert, as discussed earlier in this chapter. The researcher shall now proceed to discuss the responses obtained for

the General Principles section of the information security expert interview questionnaire.

### 8.4.2 The General Principles

The General Principles section of the questionnaire attempted to establish the extent to which the information security expert agreed with the premise on which this research study is based. In simple terms, the premise pertained to the complexity of information security best practices and standards for SA SMMEs due to the unique characteristics and constraints of SMMEs.

Moreover, the research study focused on the need for SA SMMEs to be able to establish information security requirements that are based on the unique characteristics and constraints of the enterprise. Ultimately, the information security requirements can be used to design an ISMS within an enterprise, or to guide the selection of information security controls used to secure the information assets of an enterprise. Thus, the purpose of this section also functioned as a confirmation of the validity of the premise on which this research study is based.

The information security expert agreed that an ISMS is one of the most comprehensive approaches for an organisation to manage its information security efforts (measures to protect its information assets). However, when asked whether this is true of SMMEs also, the information security expert indicated that it is almost never true for SMMEs. Elaborating on this response, the information security expert then explained that in their experience “information security management [in SMMEs] tends to be best effort but [it is] disorganised with little formal processes or structure”. This is in accordance with findings from the literature, which state that information security in most SMMEs is implemented in an ad hoc and reactive manner. Nonetheless, it was ascertained that the development of an ISMS and the selection of information security controls should be based on the unique information security requirements of that enterprise.

Pertaining to the characteristics and the constraints of SMMEs, the informa-

tion security expert was in agreement that it is usually true that SMMEs have characteristics and constraints that make them different from larger organisations. More so; these characteristics very frequently include a CEO or owner-centric (flat corporate) governance management structure. Therefore, it is not surprising, that the information security expert strongly agreed that the characteristics and constraints of SMMEs often make the implementation of information security best practices and standards a complex task for these enterprises.

According to the above discussion, it may be concluded that the information security expert is largely in agreement with the basic premise of this research study. The researcher will now continue to discuss the findings pertaining to the Draft Principles section of the questionnaire.

### **8.4.3 The Draft Principles**

The Draft Principles section of the information security expert interview questionnaire attempted to determine the extent to which the MAISRSS adheres to the draft principles derived in section 7.2 of Chapter 7.

The information security expert was in agreement that the MAISRSS is representative of the flat corporate governance management structure of most SA SMMEs. Additionally, the information security expert agreed that the MAISRSS promotes strategic alignment. In doing so, the processes of the MAISRSS show how the strategic-level (also known as the executive-level) management decisions pertaining to information security governance, are translated into information security requirements. Furthermore, the information security expert strongly agreed that the MAISRSS would allow the strategic-level management of an SMME to have insight into the decisions made within the enterprise pertaining to risk management.

Moreover, it was agreed that the processes of the MAISRSS present a simplified method for SA SMMEs to establish their information security requirements even where human resources, finance and information security expertise are scarce.

Further, it was also agreed that the information security requirements, determined by the processes of the MAISRSS, would provide sufficient metrics for SA SMMEs to measure the performance of their information security measures. Hence, the information security expert agreed again that the MAISRSS would be applicable, even as an SA SMME matures and grows.

Surprisingly, the information security expert neither agreed nor disagreed that the MAISRSS is simple enough for SA SMMEs to use without it disrupting their business operations. This response can be attributed to the elaboration that “information security governance is a challenge for all organisations, regardless of [their] size”. Lastly, the information security expert expressed that it would usually be true that the strategic management of SA SMMEs who use the processes of the MAISRSS, can claim that due diligence was done, pertaining to information security.

This concludes the discussion of the findings from the information security expert through the questionnaire. The following section will discuss how the findings of the information security expert interview were used to revise the MAISRSS.

## 8.5 Revisions to the MAISRSS

The information security expert made two recommendations to consider for the revision of the MAISRSS. Firstly, it was reported that getting information security governance right remains a challenge, regardless of the size of the organisation. Furthermore, it was suggested that ongoing owner/board involvement is the key to effectively driving information security governance in any organisation. Currently, the MAISRSS essentially involves the CEO/owner or the executive-level management of the enterprise from Enterprise Categorisation to the Information Security Directive process. Therefore, it can be argued that the ongoing involvement of the owner or manager of SMMEs is already incorporated into the MAISRSS.

The second recommendation made by the information security expert was that the cyclical nature of information security governance should be represented in the

model. Thus, the MAISRSS was revised to include arrows which indicate a cycle. This cycle shows that the processes of the MAISRSS should not be performed as a once off task. Refer to Figure 8.1 for the revised version of the MAISRSS process aspect.

**MAISRSS THE PROCESSES ASPECT**

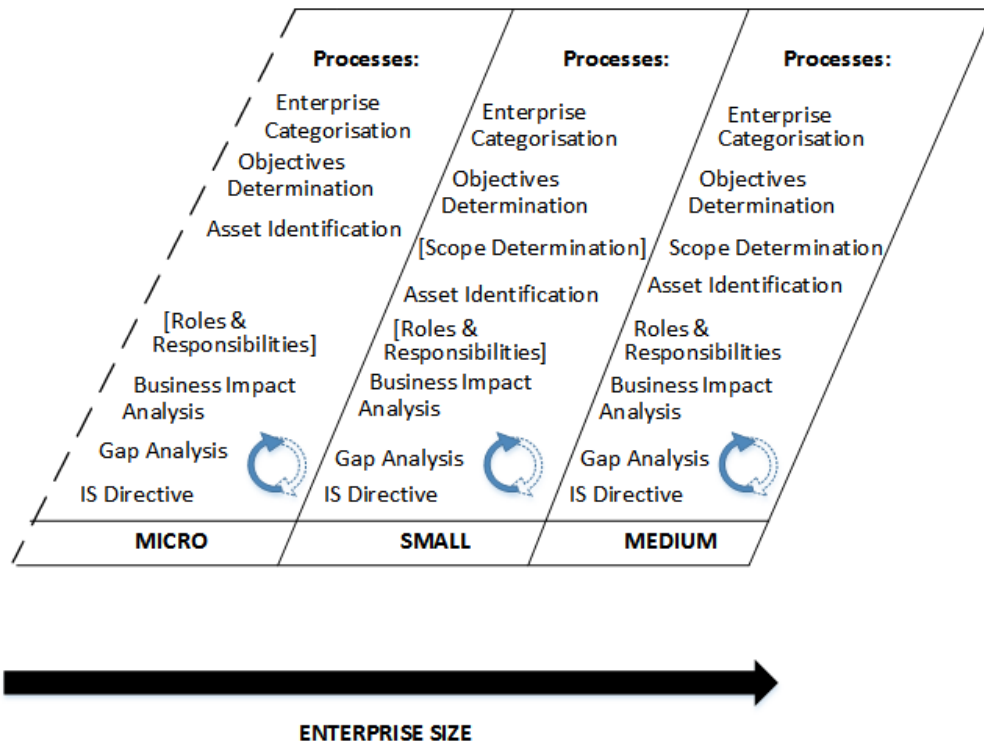


Figure 8.1: The Revised Process Aspect of the MAISRSS

## 8.6 Conclusions Drawn from the Information Security Expert Interview

Part I of this chapter discussed the questionnaire that was used as the structured interview to electronically and remotely conduct an expert interview with an information security expert. Thus, the characteristics of the ideal information security expert were set; and a section of the questionnaire was used to establish whether the respondent was an information security expert. It was confirmed that the respondent could indeed be considered an information security expert, according to this research study.

The findings of the information security expert interview indicated that to a large extent the MAISRSS adheres to the draft principles that were used to guide its design and development. Furthermore, the premise on which this research study is based was also confirmed to be valid. The premise on which this research study was based, is that information security best practices and standards are too complex for SMMEs.

Thus, the information security expert declared the MAISRSS was a “very good model”. However, the recommendations towards improvements to be made were stated and addressed, as discussed in the previous section. Therefore, it may be concluded that the MAISRSS has been validated as fit to be used by SA SMMEs in establishing their unique information security requirements.

Part II of this chapter will discuss an expert interview that was conducted with an SMME expert to evaluate the automated tool.



# Evaluating the Automated Tool

## 8.7 PART II: Designing the SMME Expert Interview

As discussed in Part II of Chapter 7, an automated tool for the alignment of information security requirements in SA SMMEs was developed. The automated tool was developed, based on the processes of the MAISRSS. In addition to demonstrating the practicality of the MAISRSS, the automated tool presented an automated version of the MAISRSS processes.

As discussed in Chapter 6, the researcher experienced a number of difficulties in obtaining responses from SA SMMEs; even after contacting small business related growth and development incubation hubs and agencies, magazines, forums and several individual SMME owner/managers. Hence, it was concluded that interviewing an expert in the SA SMME sector could prove to be a rich and sufficient source for the evaluation of the automated tool.

Thus, an expert interview was conducted with an individual considered to be an expert in the SA SMME sector. Similar to the information security expert interview, a questionnaire was sent to the SMME expert via email. A suite of information accompanied the SMME expert interview questionnaire too. This suite included background information about the research project, as well as definitions and explanations of information security governance and information security requirements. However, the information in this suite was prepared for an audience without any prior knowledge of information security governance and related terms. Thus, the discussion in this suite included in-depth definitions of information security and information security requirements, the MAISRSS and the automated tool. Once again, a video demonstration was included. This video demonstration showed how the automated tool prototype functions. Lastly, the questionnaire was added to the suite of attachments sent to the SMME expert. The questionnaire again offered a means of structured interviewing even in the absence of face to face or live correspondence. Refer to the folder named SMME Expert Interview on the compact disc, for the suite of information referred to in

this discussion.

Each of the following sections will discuss the purpose of the Background Information, the General Principles and the Draft Principles sections of the questionnaire.

### **8.7.1 The Background Information**

Similar to the information security expert interview, the SMME expert interview was not based on the academic qualifications of the respondent. The respondent was selected as an information expert based primarily on the number of years of experience in the SMME sector.

The respondents were allowed the option of providing their name and title. Additionally, the respondents were asked what their current occupation is, along with the job description of what that role entails. The core purpose of this section of the questionnaire was the number of years of experience that the respondent had been working in the SMME sector and their level of confidence in answering questions pertaining to SMMEs. Although the respondent indicated that they had no academic qualifications related to information security governance; they were not excluded on the basis of this responses. The reason for this decision is that the SMME expert only required knowledge about SMMEs, to be able to evaluate the automated tool.

The respondent was then directed to the General Principles section of the questionnaire.

### **8.7.2 The General Principles**

Once again, similar to the information security expert interview, the General Principles section attempted to establish the extent to which the expert agreed with the premise on which this research study is based. Thus, the SMME expert was asked questions pertaining to the characteristics and the constraints of SMMEs and

the involvement of the executive level management of an enterprise in information security governance.

### **8.7.3 The Draft Principles**

The Draft Principles section of the questionnaire attempted to establish the extent to which the SMME expert agreed that the automated tool adhered to the draft principles, which guided the development of the MAISRSS. Due to the background of the SMME expert not originating in the ICT or information security field, simplified questions were used. However, a link can still be seen between the draft principles and the questions in this section of the questionnaire. A copy of the questionnaire can be found at the end of this dissertation as Appendix D.

The next section of this chapter will discuss and analyse the responses obtained from the SMME expert interview.

## **8.8 Analysis and Results of the SMME Expert Interview**

This section of the chapter discusses the responses obtained from the SMME expert interview. The discussion will be divided into three sections, according to the sections of the questionnaire, as mentioned previously. Additionally, the researcher will report on the revisions made to the automated tool and the conclusions that were drawn, based on the responses of the SMME expert.

### **8.8.1 The Background Information**

Although the respondent provided his/her name, surname and title, these will not be reported on; and they were used only to inform the respondent about the progress of the research study. The respondent reported that his/her current occupation was as an operations manager. As an operations manager, the respondent was responsible for managing the daily operations of their enterprise.

Pertaining to years of experience, the SMME expert claimed to have twenty years of experience working in the SMME sector; consequently, resulting in the respondent being very confident about answering questions pertaining to SMMEs.

The respondent reported that their academic qualifications were completely unrelated to information security governance. However, the respondent strongly agreed that he/she was confident in their ability to answer questions about information security governance in their enterprise.

Having ascertained the vast number of years of experience of the respondent in the SMME sector, the respondent met the criteria to qualify as an SMME expert for the purposes of this research study. The occupation of the respondent was seen as an added benefit to the insight, which only an SMME expert could provide.

### **8.8.2 The General Principles**

Asked about the transparency in organisations pertaining to executive management directives being linked to implemented information security controls, the SMME expert strongly agreed with the need for transparency. Furthermore, the SMME expert also strongly agreed that the executive management of an enterprise should define how decisions on information security risk, are made within the enterprise.

In response to scalability, the SMME expert indicated that very frequently they have experienced that a tool needs to be scalable to various sizes and levels of maturity, in order to be of use to most SMMEs. Additionally, the SMME expert strongly agreed that the characteristics and the constraints of SMMEs require that such tools be simple. Therefore, it may be assumed that the above are the reasons for the SMME expert agreeing that most information security best practices and standards are too resource intensive for most SMMEs to use.

The SMME expert also agreed that information security requirements should be used as a metric to measure the performance of information security controls implemented by an enterprise. Asked about due diligence and SMMEs, the SMME

expert indicated that in their opinion, it is very important to prove due diligence pertaining to information security risk, in order to avoid legal liability.

A discussion of the responses obtained in the Draft Principles section of the questionnaire will follow next in this chapter.

### 8.8.3 The Draft Principles

It was recommended that the SMME expert reviews the automated demonstration video prior to answering the questions in the Draft Principles section of the questionnaire. The Draft Principles section attempts to obtain the opinion of the SMME expert on the extent to which the automated tool conforms to the draft principles, which guided the development of the MAISRSS.

Having the insight of a manager, the SMME expert was knowledgeable about most of the questions asked. The SMME expert agreed that the automated tool provided a method simple enough to determine the information security requirements of their enterprise. However, the expert remained neutral, neither agreeing or disagreeing on the automated tool being applicable in enterprises with minimal resources. This response was attributed to the comment that most SMME owners are often not even aware of their information assets, let alone the need to protect them.

About scalability, the SMME expert agreed that the automated tool is currently useful to their enterprise; and it could remain so even as the enterprise grows and matures. Furthermore, the SMME expert indicated that they are confident that the information security requirements generated by the automated tool, could be used as metrics to evaluate the performance of the information security measures implemented by an enterprise. Moreover, the SMME expert agreed that the information security requirements established through the automated tool would clearly link the need of an enterprise to the information security measures implemented based there on. Similarly, the SMME expert indicated that there is a good

link between the vision of an enterprise and its information security requirements as generated by the automated tool.

This concludes the responses of the SMME expert to the interview questionnaire. The following section will discuss the recommendations of the SMME expert for the revision of the automated tool.

## **8.9 Revisions to the Automated Tool**

The SMME expert offered no recommendations or suggestions for revising the automated tool. It was stated that the automated tool is simple to use; and that it would add value. However, it was noted that most SMME owners would not see the value of protecting their information assets if they are unaware of what information assets are. Therefore, it was suggested that information security education should be a precursor to introducing the automated tool to SMMEs. Figure 8.2 is a snapshot of the SMME expert's comments, as already discussed.

My concern is that most executive managers (generally owners) for micro / small enterprises (and many medium sized ones too) are not even aware of their information assets, let alone the need to protect them.

So, how do you convince a one-man plumber that he needs this tool or that he has information assets when many of them keep their "records" in a box under the seat of the bakkie, for example?

The return for the user in terms of reward for effort at using the tool, and maintaining the data seems minimal to most SMME's.

I have assisted many micro / small enterprises in setting up admin systems for their businesses, and cannot think of one that would even consider that they needed this tool let alone that they had information assets. The concept of information assets and how these exist in an enterprise seems problematic for small business owners.

The tool itself is simple to use and will add value. The first thing to get right is the educational component (understanding what / why / etc) for executive owners of SMME's.

Figure 8.2: Comments of the SMME Expert on the automated tool.

Although the comments of the SMME expert have been noted, information security education is beyond the scope of this research study. However, for future research, information security education can be included as a component of the MAISRSS and consequently for the automated tool also.

## 8.10 Conclusions Drawn from the SMME Expert Interview

Based on the above discussions, to a large extent, the SMME expert agreed with the General Principles, which form the premise of this research study. Thus, it may be concluded that the premise of this research study (that information security best practices and standards are too complex for SMMEs) has also been validated by an SMME expert.



Furthermore, the researcher largely agreed that the automated tool conforms to the draft principles (strategic alignment, risk control, feasibility, performance measurement, utility, simplicity, and due diligence). Therefore, it may be concluded that the automated tool has demonstrated the practical implementation of the MAISRSS processes.

## 8.11 Conclusion

In this chapter, structured interviews were discussed as the means of evaluating both the MAISRSS and the automated tool development, based on the processes of the MAISRSS. Subsequently, the researcher discussed how the structured interviews were conducted through a questionnaire by means of electronic mail.

A section of this chapter discussed the instruments that we developed to conduct the expert interviews to evaluate the MAISRSS and the automated tool. Another section of the chapter reviewed the responses obtained from the evaluation interview conducted with an information security expert. An information security expert was chosen, based on the criteria, including the number of years of experience. The information security expert evaluated the extent to which the MAISRSS adhered to the seven draft principles derived in section 7.2 of Chapter 7. To a large extent, the information security expert agreed with the questions about the MAISRSS, based on the draft principles. Thus, it was concluded that the MAISRSS has been validated as a simpler method, suitable for SA SMMEs to establish their information security requirements.

Additionally, an SMME expert was selected. The selected SMME expert had twenty years of experience working with SMMEs. Similarly, the SMME expert answered questions about the automated tool, based on the draft principles. The responses of the SMME expert resulted in the conclusion that the automated tool conformed to the draft principles on which the MAISRSS was developed. In addition, the automated tool was validated as being simple enough for SA SMMEs to use in establishing their information security requirements. Thus, it

was concluded that the automated tool demonstrated the feasibility of a practical implementation of the MAISRSS.

The following chapter, Chapter 9, will discuss how the research objectives of this research study were met.

# Chapter 9

## Conclusion

*“Now a whole is that which has a beginning, middle, and end.”*

-Aristotle

### 9.1 Introduction

This research study focused on the ability of South African (SA) small medium and micro enterprises (SMMEs), to establish their information security requirements. It was established that SMMEs in SA have similar characteristics to other SMMEs, as reported in the literature. Furthermore, these characteristics present inherent constraints that make the current implementation of information security best practices and standards too complex for SMMEs. Thus, it was determined that the research problem to be investigated by this research study reads as follows: **The unique characteristics of SMMEs make the current information security best practices and standards too complex for SA SMMEs to use in establishing the information security requirements aligned to the objectives of the enterprise.** It was therefore hypothesised that **the development of a model based on the unique characteristics of SA SMMEs, would simplify the process of establishing the information security requirements aligned to the objectives of these enterprises.**

The developed model (A Model for the Alignment of Information Security

Requirements in SA SMMEs or MAISRSS), was discussed in Chapter 7 and validated in the previous chapter (Chapter 8). With this accomplished, this chapter will conclude this dissertation by reviewing the chapters already presented and highlighting the major aspects and arguments. In doing so, the research objectives will be revisited in the appropriate section of this chapter. Thereafter, a discussion concerning how these objectives were accomplished will be provided. Finally, possible avenues of expanding research in the area of this research study will be discussed.

## 9.2 Summary of Chapters

Various chapters have contributed to the accomplishment of the research objectives of this research study. Each of the chapters addressed a specific research objective and contributed findings which culminated in the development of the MAISRSS. This section will discuss the findings of each of the preceding chapters found in this dissertation.

In **Chapter 1**, it was established that SMMEs, like most modern organisations, also require information to perform business operations. Thus, information is regarded as an asset to all organisations. Furthermore, it was reported that frequently information and communication technology (ICT) systems are used to create, store and transmit the information assets of SMMEs too. Although the ICT systems provide convenience, these systems present vulnerabilities that can be exploited by adversaries, in order to gain access to, or to sabotage enterprises' information assets. Thus, it is reported that SMMEs should determine the level of protection required to adequately protect their information assets. However, it was discovered that the unique characteristics of SMMEs present constraints, which make information security best practices and standards too complex for SMMEs. This then leads to the identification of the problem to be investigated by this research study. The research objectives of this research study and the research process that was followed, were also briefly introduced.

Information security best practices and standards offer guidance on establishing effective information security governance, according to the information security requirements of an organisation. Therefore, the outcomes of good information security governance were identified from the literature in **Chapter 2**. The six reported outcomes of good or effective information security governance were identified, as may be seen in section 2.4.5 of Chapter 2. Furthermore, the chapter explored how to direct and control (govern) information security and the advantages of using the guidance of information security best practices and standards to accomplish this.

The research problem that was addressed by this research study, as established in Chapter 1, pertains to the complexity of information security best practices and standards in SA SMMEs. Furthermore, the research problem particularly involves the use of information security best practices and standards by SA SMMEs, to establish their information security requirements. Consequently, **Chapter 3**, expanded on the concept of information security requirements by reporting on the general definition of information security requirements. Additionally, the chapter reiterated the definition found in information security best practices and standards. The perspective of various authors of literature on the definition of information security requirements was also discussed. Finally, the researcher compared two methods of establishing information security requirements namely, information security risk analysis and information security requirements analysis. Both of these methods are documented in ISO/IEC 27003 (2010).

It was first mentioned in Chapter 1 that the unique characteristics of SMMEs make these information security best practices and standards too complex. Accordingly, **Chapter 4** delved into the details of the unique characteristics of SMMEs and the constraints to the success of SMMEs. The result of this exercise was a list of core elements that should guide the design and development of any information security artefact developed for SMMEs.

Similar to most scholarly works, a formalised research design was followed throughout this research study. The research design used in this research study,

was a result of integrating design-oriented IS research and design-based research approaches, as discussed in **Chapter 5**. The various research methods used in this research study were discussed in this chapter.

The use of surveys in this research study was also discussed in Chapter 5. However, the design and the findings of one particular survey conducted in this research study were conveyed to **Chapter 6**. The purpose of the survey was to verify the validity of the core elements discovered in Chapter 4 in an SA SMME environment. Therefore, the survey of a few SA SMMEs and the findings thereof were reported on.

Subsequently, the findings of the survey together with those from the literature, resulted in the formation of draft principles that guided the development of the model as seen in **Chapter 7**. Before conducting the survey and deriving the draft principles, a theoretical model was constructed. However it was later realised that the theoretical model was not constructed according to the characteristics and constraints of SMMEs.

Consequently, the draft principles were derived and a model and automated tool were developed; which lead to two part discussion was in Chapter 7. Firstly, the researcher reported on the developed Model for the Alignment of Information Security Requirements in SA SMMEs (MAISRSS). Secondly, the development of an automated tool for the alignment of information security requirements in SA SMMEs (the automated tool) was discussed. The automated tool was developed as a proof-of-concept prototype to demonstrate the practicality of the MAISRSS.

Consequently, both the MAISRSS and the automated tool were verified. **Chapter 8**, reported on the approach used to verify the MAISRSS and the automated tool. It also presented the feedback obtained from the verification process. The reporting in this chapter also followed a two part structure. In addition to the feedback obtained, it was described how the MAISRSS would be adapted in line with the feedback. Pertaining to the automated tool, the recommendations for further improvements of the tool were presented. Thus, on the basis of the performed

evaluation, the MAISRSS was confirmed to be a sound model. Furthermore, the development and the evaluation of the automated tool prototype verified the practical relevance of the MAISRSS.

### 9.3 Problems and Challenges

Similar to most research studies, this research study was subject to limitations too. These limitations prevented the findings of this research study from being generalised to all SMMEs in SA.

One of the limitations, which posed a challenge for this research study was identifying organisations as SMMEs. SMMEs fit criteria which are not identifiable without obtaining information pertaining to the finances and the size of the workforce of an organisation. Therefore, identifying SMMEs became a difficult exercise for the researcher. Even numerous attempts over a number of months of attempting to contact SMMEs and start-up enterprises through seed funding and incubation organisations by making telephonic calls, sending sms messages, as well as e-mail requests, became a futile exercise. As mentioned in section 6.5 of Chapter 6, more than 15 small business related growth and development incubation hubs and agencies, magazines, forums (organisations affiliated to SA SMMEs) and several individual SMME owner/managers were contacted; all with no luck of willingness to participate. Consequently only nine responses to the survey were received. The nine SMME responses were too little to collect a sample significant enough to generalise the findings of the survey to the greater SMME population in SA. However, this survey endeavoured only to confirm what was already established in the literature. Thus, it may be assumed to already be known in SMMEs worldwide as common phenomenon.

The second challenge or problem presented itself in the form of a lack of participants for the verification of the automated tool. Initially, it was intended to host a workshop, in which SMME practitioners would view a demonstration of the automated tool. Alternatively, an SMME expert with 20 years of experience was

identified as the most suitable candidate to perform the evaluation, as seen in Part I of Chapter 8.

## 9.4 Summary of Contributions

ICT has modified and enhanced the manner in which organisations collect, store and transmit information. However, the vulnerabilities of ICT systems put the information (a critical asset to organisations) at risk of loss or sabotage by the adversaries. Therefore, organisations must employ methods for protecting their information assets against these risks. Thus, each organisation should establish the level of protection required for each of their information assets. These are known as information security requirements. Information security requirements and the processes to establish information security requirements are documented in the form of information security best practices and standards.

Regrettably, information security best practices and standards are too resource intensive. It was reported that most information security best practices and standards were developed for large organisations; with three-tiered corporate governance structures, work forces with a greater level of expertise and more finances. Consequently, due to their unique characteristics and constraints, such as a lack of expertise, limited financial resources and a CEO-owner-centric corporate governance structure, most SMMEs find the use of information security best practices and standards too complex. Thus, the research problem to be addressed by this research study pertained to *information security best practices and standards being too complex for SA SMMEs to implement in determining their information security requirements aligned to the objectives of the enterprise* as may be seen in section 1.6.1 of Chapter 1.

Subsequently, the research objectives were constructed to address the identified research problem. The primary research objective of this research study was *To develop a model based on the unique characteristics of SMMEs, which would simplify how SA SMMEs could establish their information security requirements*



*that are aligned to the objectives of the enterprise*, as already mentioned earlier.

Four secondary research objectives were constructed to support the accomplishment of the primary research objective. The four secondary research objectives of this research study were defined in section 1.7.2 of Chapter 1, and are they listed below:

- To identify from the literature, what the outcomes of good information security governance should be;
- To establish the criteria that define an information security requirement from the information security best practices and standards;
- To obtain the perspectives of various authors on the use and understanding of information security requirements; and
- To determine the core elements of an artefact developed for SMMEs.

Each of the secondary research objectives of this research study were accomplished in a chapter (Chapters 2 to 4) of this dissertation, where appropriate.

The discussion of the findings of the chapters of this dissertation and how they pertain to the secondary research objectives can be seen below:

Secondary research objective 1 - *to identify from the literature, what the outcomes of good information security governance are* - was addressed in Chapter 2. Through the literature review, the researcher identified six outcomes of good or effective information security governance, as may be seen in section 2.4.5 of Chapter 2. Thus, this objective was satisfactorily met.

Secondary research objective 2 - *to establish the criteria that define an information security requirement from the information security best practices and standards* - addressed in Chapter 3. This chapter reviewed the information security best practices and standards, such as: ISO/IEC 27002 (2012) and NIST SP800-53, in order

to determine what the documented sources and the structure of an information security requirement are. Therefore, this research objective was accomplished.

Secondary research objective 3 - *to obtain the perspectives of various authors on the use and the understanding of information security requirements* - This was also addressed in Chapter 3. Various published sources on information security requirements and their use were reviewed. The findings from this literature review were reported in section 3.4 of Chapter 3. This concluded the secondary research objectives addressed by this chapter, confirming that both secondary research objective 2 and 3, were satisfactorily addressed in Chapter 3.

Secondary research objective 4 - *to determine the core elements of an artefact developed for SMMEs* - as addressed in Chapter 4. Based on the characteristics and the constraints of SMMEs, together with an analysis of the literature and the reports, such as those of the European Union Agency for Network and Information Security (ENISA), the six core elements of an artefact developed for SMMEs were derived. Thus, it was concluded that the secondary research objective 4 was satisfactorily reached.

In addition to the listed objectives, a survey had to be conducted *to confirm the findings about SMMEs globally*; from the literature, in the SA SMME context also (as can be seen in Chapter 6). Furthermore, as a requirement of design-based research, *draft principles had to be derived* to guide the construction of the MAISRSS, as discussed in Chapter 7. Constructing the MAISRSS addressed the primary research objective of this study, as discussed in section 1.7 of Chapter 1. Consequently, the MAISRSS and the automated tool that was developed based on the model, had *to be evaluated* to ensure that they conform with the draft principles.

Thus, as can be seen in Part I and Part II of Chapter 8, respectively, two expert interviews were conducted to verify that the MAISRSS and the automated tool conform to the draft principles. However, it is important be cognisant of the roles of Chapter 1 in which the context of the research study was set and the

problem and research objectives were introduced; as well as Chapter 9, where it was discussed how this study accomplished its research objectives.

Owing to the discussion of the contributions of the chapters of this dissertation, as can be seen above; Chapters 2 to 8 may be mapped to a research objective and the research method(s) used to accomplish that objective (the contribution). Refer to Table 9.1, which is a summary of the contribution of each chapter of this dissertation.

<b>Research Objectives</b>	<b>Chapter</b>	<b>Research Method</b>
PO.To develop a model based on the unique characteristics of SMMEs, which would simplify how SA SMMEs establish the information security requirements that are aligned to the objectives of the enterprise.	Chapter 7 & 8	Modelling Prototyping Expert Interviews
SO1.To identify from the literature, what the outcomes of good information security governance are.	Chapter 2	Literature Review
SO2.To establish the criteria that define an information security requirement from information security best practices and standards.	Chapter 3	Literature Review
SO3.To obtain the perspective of various authors on the use and understanding of information security requirements.	Chapter 3	Literature Review
SO4.To determine the core elements of an information security artefact developed for SMMEs.	Chapter 4 & 6	Literature Review Survey Triangulation

Table 9.1: A Summary of the contribution of the chapters of this dissertation

It is evident that each of the secondary research objectives of this research study have been reached. The accomplishment of the secondary research objectives culminated in the development of the Model for the Alignment of Information

Security Requirements in South African Small, Medium and Micro Enterprises (MAISRSS). Developing the MAISRSS aligned to the primary research objective of this research study, which was to develop a model based on the unique characteristics of SMMEs, which would simplify how SA SMMEs establish their information security requirements that are aligned to the objectives of the enterprise. It can, therefore, be argued that the primary research objective of this research study has been met satisfactorily.

## 9.5 Suggestions for Future Research

This research study developed a model in an attempt to address the complexity of information security best practices and standards in establishing the information security requirements of SA SMMEs. However, too few enterprises participated in the survey for the findings of this research study to be generalised to the greater SMME population in SA. Therefore, future research work could conduct a similar study with a larger population sample.

Additionally, this research study focused only on simplifying how SA SMMEs establish their information security requirements. However, as suggested by the SMME expert in section 8.9 of Chapter 8, most SA SMMEs are unaware that they possess information assets. Furthermore, these SA SMMEs are not aware of the reward or the reason for protecting their information assets. Thus, an avenue for future research work includes information security awareness campaigns for SA SMMEs. However, this is beyond the scope of this research study and will instead be recorded as one of the design principles output by this research study.

## 9.6 Epilogue

This dissertation presented the MAISRSS, a model to address the problem of information security best practices and standards that were too complex for SA SMMEs to establish their information security requirements. The MAISRSS was developed, according to the guidance of draft principles derived from the characteristics of SA SMMEs. Subsequently, both the MAISRSS and the prototype developed from this model were evaluated and verified to be adequate to establish information security requirements and suitable for SA SMMEs.

# References

- Abor, J., & Adjasi, C. K. (2007). Corporate governance and the small and medium enterprises sector: theory and implications. *Corporate Governance: The international journal of business in society*, 7(2), 111–122.
- Abor, J., & Biekpe, N. (2007). Corporate governance, ownership structure and performance of SMEs in Ghana: implications for financing opportunities. *Corporate Governance*, 7(3), 288–300.
- ACCA. (2015). *Governance for all: the implementation challenge for SMEs* (Tech. Rep.). London: Association of Chartered Certified Accountants.
- Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). OCTAVE-S Implementation Guide. *Software Engineering Institute*, 1(V 1.0), 1–63.
- Amsenga, J. (2008). An introduction to standards related to information security. *Security*, 243–258.
- Anderson, T., & Shattuck, J. (2012). Feature Articles. 41(1), 16–25.
- Andress, J. (2014). *The Basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). United States of America: Elsevier.
- Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. *International Journal of Information Science and Management*, 11(SPL.ISS.), 111–126.

- Ayat, M., Masrom, M., Sahibuddin, S., & Sharifi, M. (2011). Issues in implementing IT governance in Small and Medium Enterprises. *Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011*, 197–201.
- Banham, H., & He, Y. (2010). SME Governance: Converging Definitions And Expanding Expectations. *The International Business & Economics Research Journal*, 9(2), 77–82.
- Barab, S., & Squire, K. (2004). Design-Based Research : Putting a Stake in the Ground Design-Based Research : Putting a Stake in the Ground. *Journal of the Learning Sciences*, 13(1), 1–14.
- Barlette, Y., & Fomin, V. V. (2008). Exploring the suitability of IS security management standards for SMEs. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10.
- Barlette, Y., & Fomin, V. V. (2010). The Adoption of Information Security Management Standards. *Cyber Security and Global Information Assurance*, 119–140.
- Baskerville, R., & Siponen, M. (2002). An information security metapolicy for emergent organizations. *Logistics Information Management*, 15(5/6), 337–346.
- Beaver, G., & Prince, C. (2004). Management, strategy and policy in the UK small business sector: a critical review. *Journal of Small Business and Enterprise Development*, 11(1), 34–49.
- Benbasat, I., & Zmud, R. W. (1999). EMPIRICAL RESEARCH IN INFORMATION SYSTEMS : THE PRACTICE OF RELEVANCE ^ The Nature of Relevant. *MIS Quarterly*, 23(1), 3–16.
- BER. (2016). The small, medium and micro enterprise sector of south africa. (1), 1–35.



- Beranek, L. (2011). Risk analysis methodology used by several small and medium enterprises in the Czech Republic. *Information Management & Computer Security*, 19(1), 42–52.
- Bhattacharya, D. (2008). Leadership styles and information security in small businesses: An empirical investigation. *Information Security*(April), 1–251.
- Bogner, A., Beate, L., & Menz, W. (Eds.). (2009). *Research Methods Series: Interviewing Experts*. London: Palgrave Macmillan.
- Boubala, H. G. (2010). *Risk management of SMMEs*. Doctoral dissertation, Cape Peninsula University of Technology.
- Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, 11(1), 26–31.
- Brotby, K. (2009). *INFORMATION SECURITY GOVERNANCE INFORMATION SECURITY GOVERNANCE A Practical Development and Implementation Approach*. New Jersey: John Wiley & Sons, Inc.
- Burns, A., Davies, A., & Davies, P. B. (2006). A study of the uptake of information security policies by small and medium sized businesses in wales. *Proceedings of the International Conference on Electronic Business (ICEB)*.
- Calder, A. (2009). *A Management Guide: Implementing Information Security based on ISO 27001/ ISO 27002* (2 ed.). London: Van Haren Publishing.
- Checkland, P., & Poulter, J. (2010). Soft Systems Methodology. In M. Reynolds & S. Holwell (Eds.), *Systems approaches to managing change: A practical guide* (pp. 191–242). Lancaster: The Open University.
- Chitu, O., & Schabram, K. (2010). A guide to conducting systematic literature review of information systems research.
- Clarke, R. (2015). The prospects of easier security for small organisations and consumers. *Computer Law and Security Review*, 31(4), 538–552.

- Coertze, J., & Von Solms, R. (2013). A software gateway to affordable and effective Information Security Governance in SMMEs. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*.
- Creative Research Systems. (2012). *Sample Size Calculator*. (<https://www.surveysystem.com/sscalc.htm>[surveysystem.com](https://www.surveysystem.com)[Online; posted August-2012 accessed May-2017])
- D'Arcy, J., Herath, T., Shoss, M. K., D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318.
- Delpont, P. M., Von Solms, R., & Gerber, M. (2015). Good corporate governance of ICT in municipalities. *2015 IST-Africa Conference, IST-Africa 2015*, 152(1), 1–10.
- Delpont, P. M. J. (2017). A Framework for the Corporate Governance of ICT in Local Government. *unpublished:dissertation*.
- Devos, J., Van Landeghem, H., & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. *Industrial Management & Data Systems*, 112(2), 206–223.
- Dhillon, G., Stahl, B. C., & Baskerville, R. (2009). Creativity and Intelligence in Small and Medium Sized Enterprises : The Role of Information Systems. *Ifip International Federation For Information Processing*, 1–9.
- Dojkovski, S., Lichtenstein, S., & Warren, M. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. *Ecis*(2007), 1560–1571.
- DTI. (2006). *Information security : Protecting Your Business Assets* (Tech. Rep.). London: Department of Trade and Industry.

- Dube, I., Dube, D., & Mishra, P. (2011). Corporate Governance Norm for SME. *Journal of Public Administration and Governance*, 1(2), 77.
- Eco, U. (2015). *How to Write a Thesis*. Cambridge, Massachusetts: The MIT Press.
- ENISA. (2016). *Guidelines for SMEs on the security of personal data processing* About ENISA Guidelines for SMEs on the security of personal data processing. London: European Union Agency for Network and Information Security (ENISA).
- Ernest Chang, S., & Ho, C. B. (2006). *Organizational factors to the effectiveness of implementing information security management* (Vol. 106).
- Feagin, R. D. (2015). *the Value of Cyber Security in Small Business*. Master of science in cybersecurity, Utica College.
- Fenz, S., Plieschnegger, S., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. *Information and Computer Security*, 24(5), 452–473.
- Fink, A. (2005). *Conducting Literature Reviews: From the Internet to Paper* (2nd ed.). USA: Sage Publications Ltd.
- Gable, G. G. (1994). Integrating Case study and survey research methods: an example in information systems. *European Journal of Information Systems*, 3(2), 112–126.
- Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, 277–300.
- Gerber, M. (2001). The Development of a Technique to Establish the Security Requirements of an Organization.

- Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*, 16–30.
- Gerber, M., & von Solms, R. (2008). Information security requirements Interpreting the legal aspects. *Computers & Security, 124–135*.
- Gerber, M., von Solms, R., & Overbeek, P. (2001). Information Management & Computer Security Formalizing information security requirements. *Information Management & Computer Security Iss Information Management Computer Security Iss Industrial Management & Data Systems Iss Information Management & Computer Security Iss, 9(17)*, 32–37.
- Goucher, W. (2011). Do SMEs have the right attitude to security? *Computer Fraud and Security, 2011(7)*, 18–20.
- Gupta, A., & Hammond, R. (2005). Information Management & Computer Security Information systems security issues and decisions for small businesses: An empirical examination”Information systems security issues and decisions for small businesses”. *Information Management & Computer Security Information Management Computer Security Iss Industrial Management & Data Systems, 13(3)*, 297–310.
- Hancock, D. R., & Algozzine, B. (2011). *Doing Case Study Research: A practical Guide for Beginning Researchers* (Second ed.). Teachers College Press, 1234 Amsterdam Avenue, New York, NY 10027.
- Hankinson, A., Bartlett, D., & Ducheneaut, B. (1997). The key factors in the small profiles of smallmedium enterprise ownermanagers that influence business performance: The UK (Rennes) SME survey 19951997 An international research project UK survey. *International Journal of Entrepreneurial Behavior & Research, 3(3)*, 168–175.
- Herrington, J., Mckenney, S., Reeves, T. C., Oliver, R., Herrington, J., & Mckenney, S. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In C. Montgomerie & J. Seale (Eds.),

*World conference on educational multimedia, hypermedia and telecommunications* (pp. 4089–4097). Chesapeake, VA: Edit Cowan University.

Herrmann, P., & Herrmann, G. (2006). Security requirement analysis of business processes. *Electronic Commerce Research*.

Hofstee, E. (2009). *Constructing a Good Dissertation*. Sandton, Johannesburg: EPE Publishers.

Hutchinson, D., Armitt, C., & Edwards-Lear, D. (2014). The application of an agile approach to it security risk management for SMES. *Proceedings of 12th Australian Information Security Management Conference, AISM 2014*, 82–90.

Huysamen, G. K. (1998). *Descriptive statistics for the social and behavioural sciences*. van Schaik.

Institute of Directors in Southern Africa. (2009a). *Governance in SMEs* (Tech. Rep.). Johannesburg: Institute of Directors Southern Africa.

Institute of Directors in Southern Africa. (2009b). King Code of Governance for South Africa 2009. *King Report on Governance for South Africa 2009*, 66.

Isaca. (2012). *COBIT 5 for information security* (Tech. Rep.). Illinois, IL: Information Systems Audit and Control Association.

*ISO/IEC27000:2012 Information technology Security techniques Information security management systems Overview and vocabulary* (2 ed.). (2012). Switzerland: International Organization for Standardization/the International Electrotechnical Commission.

ISO/IEC27001. (2013). *ISO/IEC27001:2013 Information technology Security techniques Information security management systems Requirements* (Tech. Rep.). Switzerland: International Organization for Standardization/the International Electrotechnical Commission.

- ISO/IEC27002, & ISO/IEC27001. (2013). *ISO/IEC27002:2013 Information technology Security techniques Information security management systems Requirements* (Tech. Rep.). Switzerland: International Organization for Standardization/the International Electrotechnical Commission.
- ISO/IEC27003. (2010). *ISO/IEC 27003 : 2010 Information technology Security techniques Information security management system implementation guidance* (1 ed.). Switzerland: International Organization for Standardization/International Electrotechnical Commission.
- ISO/IEC27005. (2011). *ISO/IEC 27005 : Information technology Security techniques Information security management systems Requirements* (Tech. Rep.). Switzerland: International Organization for Standardization/ International Electrotechnical Commission.
- ISO/IEC38500. (2015). *ISO/IEC38500:2015 Information technology - Governance of IT for the organization* (2 ed.). Switzerland: International Organization for Standardization/International Electrotechnical Commission.
- ITGI, & OGC. (2008). *Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit-res\_Eng\_1108* (Tech. Rep.). IT Governance Institute, Office of Government Commerce.
- Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R. A., Mashal, F. A., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical and Industrial Engineering*, 8(2), 102–118.
- Kajornboon, A. (2005). Using interviews as research instruments. *E-journal for Research Teachers*, 2(1), 1–9.
- Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139–154.

- King Committee. (2016). King IV Report on Corporate Governance for South Africa 2016. *King IV*, 1–120.
- Koornhof, H. (2009). *A Framework for IT Governance in Small Businesses*. Magister technologiae, Nelson Mandela Metropolitan University.
- Krishna, M. (2010). A Methodology for Measuring Information Security Maturity in Norwegian and Indian MSME's with special focus on people factor.
- Lakshminarayanan, V., Liu, W., Chen, C. L., Easterbrook, S., & Perry, D. E. (2006). Software architects in practice: Handling requirements. In *Proceedings of the 2006 conference of the center for advanced studies on collaborative research* (p. 25). IBM Corp.
- Laksono, H., & Supriyadi, Y. (2015). Design and Implementation Information Security Governance Using Analytic Network Process and COBIT 5 For Information Security A Case Study of Unit XYZ. *2015 International Conference on Information Technology Systems and Innovation (ICITSI)*(1), 16–19.
- Levy, M. (2009). An exploration of the role of information systems in developing strategic growth in small and medium-sized enterprises. *Knowledge Creation Diffusion Utilization*, 1–16.
- Lin, L., Nuseibeh, B., Ince, D., Jackson, M., & Moffet, J. (2003). Introducing abuse frames for analysing security requirements. In *Proceedings of the 11th ieee international* (pp. 371–372).
- Manhart, M., & Thalmann, S. (2013). An integrated risk management framework: measuring the success of organizational knowledge protection. (July 2012), 1–7.
- Mason, J. (2002). *Qualitative Researching* (2nd ed.). Wiltshire: Sage Publications Ltd.

- Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing sme information security maturity. *Journal of Computer Information Systems*, 56(2), 106–115.
- Myagmar, S., Lee, A., & Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *Symposium on requirements engineering for information security (sreis)* (pp. 1–8).
- Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, 21(June), 1–18.
- Ngura, S., Kimwele, M., & Rotich, G. (2015). Determinants of Information Security among Small and Medium Enterprises in Kenya. *European Journal of Business Management*, 2(1), 1–20.
- NISTIR7621. (2009). Small Business Information Security : The Fundamentals Small Business Information Security : The Fundamentals. *National Institute of Standards and Technology Interagency Report*, 7621, 20.
- NISTSP800-53. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg.
- Njenga, K., & Jordaan, P. (2016). The African Journal of Information Systems We Want To Do It Our Way: The Neutralisation Approach to Managing Information Systems Security by Small Businesses We Want To Do It Our Way: The Neutralization Approach to Managing Information Systems Security by. *The African Journal of Information Systems Article*, 8(1), 42–1936.
- OECD. (2015). *Corporate-Governance-Principles-ENG* (Tech. Rep.). Ankara: Organisation for Economic Co-Operation and Development.
- Olivier, M. S. (2009). *Information Technology Research 3* (3rd ed.). Pretoria: van Schaik.



- Ongori, H., & Migiro, S. O. (2010). Information and communication technologies adoption in SMEs: literature review. *Journal of Chinese Entrepreneurship*, 2(1), 93–104.
- 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*(October), 1–4.
- Österle, P. H., & Otto, B. (2010). A Method for Researcher-Practitioner Collaboration in Design-Oriented IS Research. *Business and Information Systems Engineering*, 283–293.
- Oxford University Press. (2007). *Oxford Mini School Dictionary* (2nd ed.). New York, NY: Oxford University Press.
- Peltier, T. R. (2005). *Information Security Risk Analysis* (2nd ed.). Boca Raton, FL: Taylor & Francis Group.
- Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*(23), 638–646.
- Rasouli, M. R., Trienekens, J. J. M., Kusters, R. J., & Grefen, P. W. (2016). Information governance requirements in dynamic business networking. *Industrial Management & Data Systems*, 116(7), 1356–1379.
- Rattray, J., & Jones, M. (2007). Essentials of questionnaire design and development. *Journal of clinical nursing*, 16(2), 234–243.
- Raynard, P., Forstater, M., & UNIDO. (2002). *Corporate social responsibility: Implications for small and medium enterprises in developing countries* (Tech. Rep.). Vienna: United Nations Industrial Development Organization.
- Sánchez, L. E., Ruiz, C., Fernández-Medina, E., & Piattini, M. (2010). Managing the asset risk of SMEs. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 60, 422–429.

- Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piattini, M. (2009). Management of scorecards and metrics to manage security in SMEs. *Proceeding of the first international workshop on Model driven service engineering and data quality and security - MoSE+DQS '09*, 9.
- Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, 46(5), 267–270.
- Smit, Y., Watkins, J. A., & Yolande Smit. (2012). A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African Journal of Business Management*, 6(21), 8233.
- Spears, J. L. (2005). A holistic risk analysis method for identifying information security risks. *Security management, integrity and internal control in information systems*, 185–202.
- Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing Information Security in Small and Medium Sized Enterprises: A holistic approach. *Proceedings of the ISSE/SECURE*, 1–11.
- Thalman, S., Bachlechner, D., Demetz, L., & Maier, R. (2012). Challenges in cross-organizational security management. *Proceedings of the Annual Hawaii International Conference on System Sciences*(January 2015), 5480–5489.
- The President's Office. (1996). *No. 102 of 1996: National Small Business Act, 1996*. (No. 1901).
- Tipton, H. F., & Krause, M. (Eds.). (2006). *Information Security Management Handbook* (2006 ed.). New York, NY: Taylor & Francis Group.
- Tomhave, B. L. (2005). Alphabet soup: Making sense of models, frameworks, and methodologies. *George Washing University*.
- Upfold, C. T. (2005). An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape Research Dissertation.

- Valli, C., Martinus, I., & Johnstone, M. (2014). Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business. *Proceedings of the International Conference on Security and Management (SAM)*, 1–5.
- Van Niekerk, L., & Labuschagne, L. (2006). The PECULIUM model: information security risk management for the south african SMME. *International Information Security South Africa*, 1–14.
- Vermeulen, C., & Von Solms, R. (2002). The information security management toolbox taking the pain out of security management. *Information Management & Computer Security*, 10(3), 119–125.
- Verschuren, P., & Hartog, R. (2005). Evaluation in design-oriented research. *Quality and Quantity*, 39(6), 733–762.
- Von Solms, R., Thomson, K. L., & Maninjwa, M. (2011). Information security governance control through comprehensive policy architectures. In *Information security south africa (issa)* (pp. 1–6). Johannesburg: IEEE.
- von Solms, R., & von Solms, S. H. (2006). Information Security Governance: A model based on the Direct-Control Cycle. *Computers and Security*, 25(6), 408–412.
- von Solms, R., & von Solms, S. H. (2008). *Information Security Governance* (1 ed.). Johannesburg: Springer Publishing Incorporated.
- Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *South African Institute for Computer Scientists and Information Technologists*, 95–103.
- Whitman, M., & Mattord, H. (2012). *Principles of Information Security* (4 ed.). Boston, MA: Course Technology Cengage Learning.
- Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational

- Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, 39(2), 497–518.
- Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4), 360–365.
- Zuppo, C. M. (2012). Defining ICT in a Boundaryless World: The Development of a Working Hierarchy. *International Journal of Managing Information Technology (IJMIT)*, 4(3), 13–22.

**Part I**

**Appendices**

# Appendix A

## National Small Business Act of 1996 Schedule

## Short title and commencement

22. This Act is called the *National Small Business Act, 1996*, and comes into operation on a date fixed by the President by proclamation in the Gazette.

## SCHEDULE

(See definition of "small business" in section 1)

Sector or sub-sectors in accordance with the Standard Industrial Classification	Size or class	Total full-time equivalent of paid employees	Total annual turnover	Total gross asset value (fixed property excluded)
		<i>Less than:</i>	<i>Less than:</i>	<i>Less than:</i>
<b>Agriculture</b>	Medium	100	R 4.00 m	R 4.00 m
	Small	50	R 2.00 m	R 2.00 m
	Very small	10	R 0.40 m	R 0.40 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Mining and Quarrying</b>	Medium	200	R30.00 m	R18.00 m
	Small	50	R 7.50 m	R 4.50 m
	Very small	20	R 3.00 m	R 1.80 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Manufacturing</b>	Medium	200	R40.00 m	R15.00 m
	Small	50	R10.00 m	R 3.75 m
	Very small	20	R 4.00 m	R 1.50 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Electricity, Gas and Water</b>	Medium	200	R40.00 m	R15.00 m
	Small	50	R10.00 m	R 3.75 m
	Very small	20	R 4.00 m	R 1.50 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Construction</b>	Medium	200	R20.00 m	R 4.00 m
	Small	50	R 5.00 m	R 1.00 m
	Very small	20	R 2.00 m	R 0.40 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Retail and Motor Trade and Repair Services</b>	Medium	100	R30.00 m	R 5.00 m
	Small	50	R15.00 m	R 2.50 m
	Very small	10	R 3.00 m	R 0.50 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Wholesale Trade,</b>	Medium	100	R50.00 m	R 8.00 m

<b>Commercial Agents and Allied Services</b>	Small	50	R25.00 m	R 4.00 m
	Very small	10	R 5.00 m	R 0.50 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Catering, Accommodation and other Trade</b>	Medium	100	R10.00 m	R 2.00 m
	Small	50	R 5.00 m	R 1.00 m
	Very small	10	R 1.00 m	R 0.20 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Transport, Storage and Communications</b>	Medium	100	R20.00 m	R 5.00 m
	Small	50	R10.00 m	R 2.50 m
	Very small	10	R 2.00 m	R 0.50 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Finance and Business Services</b>	Medium	100	R20.00 m	R 4.00 m
	Small	50	R10.00 m	R 2.00 m
	Very small	10	R 2.00 m	R 0.40 m
	Micro	5	R 0.15 m	R 0.10 m
<b>Community, Social and Personal Services</b>	Medium	100	R10.00 m	R 5.00 m
	Small	50	R 5.00 m	R 2.50 m
	Very small	10	R 1.00 m	R 0.50 m
	Micro	5	R 0.15 m	R 0.10 m



# Appendix B

## A Survey of SA SMMEs

As mentioned in Chapter 6, a survey of SA SMMEs was conducted. The purpose of the survey was to confirm the findings from literature about SMMEs globally. Numerous attempts were made to contact SMME incubation hubs, magazines among others, as was discussed in Chapter 6. Below are two examples of letters of participation, which were sent to SMME incubation hubs and the questionnaire that the participants had to complete. The Appendices in this section are:

1. A letter for participation request sent to ECITI (B.1)
2. A letter for participation request sent to Propella (B.2)
3. The SMME Survey Questionnaire (B.3)

### **B.1 Request for Participation: The ECITI**

A letter of request for participation was sent to the Eastern Cape Information Technology Initiative, which is an SMME incubation hub situated in East London. Below is the letter that was sent via email.

13 September 2017

To whom it may concern:

**Request for permission to conduct research**

My name is Timothy Speckman, and I am a second year Master in Information Technology student at the Nelson Mandela University in Port Elizabeth. The research I wish to conduct for this Master's research study involves the alignment of information security requirements within South African Small, Medium and Micro Enterprises (SMME). This research study will be conducted under the supervision of Professor Mariana Gerber (Nelson Mandela University, South Africa).

The aim of the research study is to develop a simplified model to assist South African SMMEs in understanding their unique information security requirements/needs to help them with information security, i.e. to adequately protect their business' information assets against risks, thereby promoting the continued existence and sustainability of the SMME.

We have consulted the website of the Eastern Cape Information Technology Initiative (ECITI) and found that some of the strategic goals of ECITI align with the objective of this research study. Both focus on SMMEs. ECITI promotes ICT infrastructure roll-out to rural and underserved areas; however, this research study extends further to the protection of information-related Information Technology assets. Further, the outcome of this research study could support entrepreneurs in building more efficient and effective enterprises, by helping SMMEs with understanding their unique information security requirements/needs which could ultimately promote corporate governance of ICT.

Thus, we have identified SMMEs associated with the ECITI as suitable participants for this research study.



## Research Plan and Method

This research project intends to identify and incorporate the unique characteristics of SMMEs. To understand these characteristics, a survey was designed to gather an understanding of the characteristics of South African SMMEs from an information security governance perspective.

The survey is presented in the form of 27 questions, which take approximately 30 to 35 minutes to complete and can be accessed online, by following this link <https://www.esurveycreeator.com/s/2e3f65d>. The survey is available online until the 25th of September 2017. Only one member from each enterprise should complete the survey. This member can either be the enterprise owner or manager, or an individual who is responsible for the ICT or information security of the enterprise. Permission will be sought from the enterprises prior to their participation in the research. All data collected will be treated in strictest confidence and enterprises will not be identifiable in any reports that are written, as the survey respondent will remain anonymous at all times. Reports on the data collected will reflect only aggregate values. Only the researcher and supervisor will have access to the data obtained, as no information will be disclosed to any third party that is not part of this study. Participants may withdraw from the study at any time without penalty. Data to be collected pertains to the information security of the enterprise, but cannot be tied to any specific enterprise, therefore making it of a less sensitive nature.

I am hereby seeking your permission to conduct the survey on the enterprises under the incubation of the ECITI. What we ask of the ECITI, is for the distribution of the survey link and the encouragement of enterprises under their incubation to participate in the survey. In addition, I am also seeking the permission and assistance of the ECITI to arrange a meeting with willing representatives of these enterprises, at a later stage during the research study. The purpose of this meeting will be to demonstrate the model and accompanying tool to the representatives of the enterprises, in a bid to determine its relevance to the SMME sector.

Permission will be sought from the enterprises prior to their participation in the research, by means of an email inviting them to participate in the survey and/or the meeting. Enterprises are welcome to accept or decline this invitation as they please. However, the assistance of an authoritative figure such as the ECITI will increase the chances of the enterprises participating in the study.



**NELSON MANDELA**  
UNIVERSITY

Upon completion of the study, the ECITI could be provided with a copy of the research report, if necessary. The enterprises could also make use of the draft tool that will accompany the model developed as part of this research project. If you require any further information, please do not hesitate to contact us. Thank you for your time and consideration in this matter.

Your support will be highly appreciated.

Yours sincerely,

Mr Timothy Speckman and Prof. Mariana Gerber  
School of Information and Communication Technology

**Researcher**

Timothy Speckman  
s212455710@live.nmmu.ac.za  
078 773 1195

**Supervisor**

Prof. Mariana Gerber  
Mariana.Gerber@nmmu.ac.za  
+27 (0) 41 504 3705  
+27 (0) 41 504 3313 (Fax)



**A FRAMEWORK FOR THE ALIGNMENT OF INFORMATION SECURITY  
REQUIREMENTS WITHIN SOUTH AFRICAN SMALL, MEDIUM AND MICRO  
ENTERPRISES**

**Eastern Cape Information Technology Initiative  
Permission Form**

I give support to the application for the above mentioned study.

I have read the letter explaining the purpose of the research project and understand that:

- The role of the participants is voluntary.
- Enterprises will be invited to participate.
- Participants may decide to withdraw from the study at any time without penalty.
- All information obtained will be treated in strictest confidence.
- The enterprises' names will not be identifiable in any written reports about the study.
- A report of the findings will be made available to the Eastern Cape Information Technology Initiative, if required.
- Further information on the project can be sought from Mr Timothy Speckman / Prof. Mariana Gerber.

\_\_\_\_\_  
Executive Manager

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Please return to: Prof Mariana Gerber / Mr Timothy Speckman

**Researcher**

Timothy Speckman  
s212455710@live.nmmu.ac.za  
078 773 1195

**Supervisor**

Prof. Mariana Gerber  
Mariana.Gerber@nmmu.ac.za  
+27 (0) 41 504 3705  
+27 (0) 41 504 3313 (Fax)



## **B.2 Request for Participation: Propella**

A similar letter was sent to the Propella Business Hub in Port Elizabeth, which is also an SMME incubation development hub. Similar to the letter sent to the ECITI, the researcher and the study were introduced. The letter can be seen below.

3 August 2017

To whom it may concern:

**Request for permission to conduct research**

My name is Timothy Speckman, and I am a second year Master in Information Technology student at the Nelson Mandela University in Port Elizabeth. The research I wish to conduct for this Master's research study involves the alignment of information security requirements within South African Small, Medium and Micro Enterprises (SMME). This research study will be conducted under the supervision of Professor Mariana Gerber (Nelson Mandela University, South Africa).

The aim of the research study is to develop a simplified model to assist South African SMMEs in understanding their unique information security requirements/needs to help them with information security, i.e. to adequately protect their business' information assets against risks, thereby promoting the continued existence and sustainability of the SMME.

We consulted Propella Business Incubation's website and found that Propella's vision of leveraging its expertise and resource network to positively impact economic development and community wealth in Nelson Mandela Bay, is aligned with this research study. Although this study aims to develop a tool that can be used by South African SMMEs as a whole, and not only those in Nelson Mandela Bay, the output ultimately aims to provide much needed expertise to these enterprises. Further, the outcome of this research study could support entrepreneurs in building more efficient and effective enterprises, by helping SMMEs with understanding their information security requirements/needs which could ultimately promote corporate governance of ICT.

Thus, we have identified SMMEs associated with Propella as suitable participants for this research study.



## Research Plan and Method

This research project intends to identify and incorporate the unique characteristics of SMMEs. To understand these characteristics, a survey was designed to gather an understanding of the characteristics of South African SMMEs, regarding the governance of information security.

The survey is presented in the form of 27 questions, which take approximately between 30 and 35 minutes to complete and can be accessed online, by following this link <https://www.esurveycreator.com/s/2e3f65d>. The survey is available online until the 25th of September 2017. Only one member from each enterprise should complete the survey. This member can either be the enterprise owner or manager, or an individual who is responsible for the ICT or information security of the enterprise. Permission will be sought from the enterprises prior to their participation in the research. All data collected will be treated in strictest confidence and enterprises will not be identifiable in any reports that are written, as the survey respondent will remain anonymous at all times. Reports on the data collected will reflect only aggregate values. Only the researcher and supervisor will have access to the data obtained, as no information will be disclosed to any third party that is not part of this study. Participants may withdraw from the study at any time without penalty. Data to be collected pertains to the information security of the enterprise, but cannot be tied to any specific enterprise, therefore making it of a less sensitive nature.

I am hereby seeking your permission to conduct the survey on the enterprises under the incubation of Propella. What we ask of the Propella, is for the distribution of the survey link and the encouragement of enterprises under their incubation to participate in the survey. In addition, I am also seeking the permission and assistance of the Propella to arrange a meeting with willing representatives of these enterprises. The purpose of this meeting will be to demonstrate the model and accompanying tool to the representatives of the enterprises, in a bid to determine its relevance to the SMME sector.

Permission will be sought from the enterprises prior to their participation in the research, by means of an email inviting them to participate in the survey and/or the demonstration meeting. Enterprises are welcome to accept or decline this invitation as they please. However, we feel that the assistance of an authoritative figure such as Propella will increase the chances of the enterprises participating in the study.





# NELSON MANDELA

UNIVERSITY

Upon completion of the study, Propella could be provided with a copy of the research report, if necessary. The enterprises could also make use of the tool that will accompany the model developed as part of this research project. If you require any further information, please do not hesitate to contact us. Thank you for your time and consideration in this matter.

Your support will be highly appreciated.

Yours sincerely,

Mr Timothy Speckman and Prof. Mariana Gerber  
School of Information and Communication Technology

**Researcher**

Timothy Speckman  
s212455710@live.nmmu.ac.za  
078 773 1195

**Supervisor**

Prof. Mariana Gerber  
Mariana.Gerber@nmmu.ac.za  
+27 (0) 41 504 3705  
+27 (0) 41 504 3313 (Fax)



**A FRAMEWORK FOR THE ALIGNMENT OF INFORMATION SECURITY  
REQUIREMENTS WITHIN SOUTH AFRICAN SMALL, MEDIUM AND MICRO  
ENTERPRISES**

**Propella Business Incubator**  
Permission Form

I give support to the application for the above mentioned study.

I have read the letter explaining the purpose of the research project and understand that:

- The role of the participants is voluntary.
- Enterprises will be invited to participate.
- Participants may decide to withdraw from the study at any time without penalty.
- All information obtained will be treated in strictest confidence.
- The enterprises' names will not be identifiable in any written reports about the study.
- A report of the findings will be made available to the Propella, if required.
- Further information on the project can be sought from Mr Timothy Speckman / Prof. Mariana Gerber.

\_\_\_\_\_  
Executive Manager

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Please return to: Prof Mariana Gerber / Mr Timothy Speckman

**Researcher**

Timothy Speckman  
s212455710@live.nmmu.ac.za  
078 773 1195

**Supervisor**

Prof. Mariana Gerber  
Mariana.Gerber@nmmu.ac.za  
+27 (0) 41 504 3705  
+27 (0) 41 504 3313 (Fax)



Responses from both the ECITI and Propella were not of assistance in obtaining more responses to the survey.

### **B.3 The Survey: Questionnaire**

Although the above mentioned were not of assistance, the research was able to get nine responses to the survey by contact individual SMME owners directly. Below is an example of the cover letter of the survey, followed by the questionnaire that was used to gather the data from the respondents. The survey was conducted by means of an online tool, however the online tool is not show below, only a manual versions of the questionnaire is shown.

Dear Sir/Madam

RE: Research project linked to questionnaire below.

The research project, titled *A Framework for the Alignment of Information Security Requirements within South African SMMEs*, aims to assist South African SMMEs in determining the level of information security that they require to adequately protect their information assets.

SMMEs (Small, Micro and Medium Enterprises), are said to have a lack of resources, leading to them being unable to afford expertise, time and other resources required to implement proper information security. It is further alleged that information security best practices and standards are too complex and costly for SMMEs to implement as part of their information security efforts.

These information security best practices and standards provide SMMEs with guidance on the implementation of information security and the selection of information security controls. It is suggested that the organizations customize the implementation of these best practices and standards to their specific needs.

Therefore this project aims to simplify this process of organizations establishing how much information security they need, in order to efficiently and effectively customize the information security best practices and standards to their needs.

This survey attempts to verify the constraints and characteristics of SMMEs identified in literature. The survey also attempts to understand the organizational structure of these SMMEs, the challenges they face in implementing information security best practices and standards, and what a simplified framework for SMMEs should consider.

I hope that this clarifies the purpose of the questionnaire and clearly states the objective of this research project.

Timothy Speckman (Mr.)  
s212455710@nmmu.ac.za

**A framework for the alignment of information security requirements within**

**South African SMMEs Survey 2017**

**Enterprise Classification**

1. Is your organisation, or the head office of your organisation situated in South Africa?
  - a. Yes
  - b. No
2. If you answered yes to question one, which South African province is your organisation or the head office of your organisation situated in?
  - a. Eastern Cape
  - b. Free State
  - c. Gauteng
  - d. KwaZulu-Natal
  - e. Limpopo
  - f. Mpumalanga
  - g. Northern Cape
  - h. North West
  - i. Western Cape
3. Please specify your role, or occupation in the organisation.

4. What is your highest qualification, including any certifications?

Timothy Speckman 212455710

M. IT Research Survey

2017

5. Is your enterprise/organisation part of a franchise or chain store organisation?
  - a. Yes
  - b. No
6. Which of the following economic sectors/sub-sectors does your organisation belong to?
  - a. Agriculture
  - b. Mining & Quarrying
  - c. Manufacturing
  - d. Electricity, Gas & Water
  - e. Construction
  - f. Retail & Motor Trade and Repair Services
  - g. Wholesale Trade, Commercial Agents & Allied Services
  - h. Catering, Accommodation & other Trade
  - i. Transport, Storage & Communications
  - j. Finance & Organisation Services
  - k. Community, Social & Personal Services
  - l. Other (please specify): Software Engineering; Fashion Design; Healthcare Services; Arts and Culture; Print & Graphic Design (Media).
7. How many full-time, paid employees does your organisation currently employ?
  - a. 0-5
  - b. 6-10
  - c. 11-20
  - d. 21-30
  - e. 31-50
  - f. 51-200
  - g. 200 or more
8. What is the average annual turnover of your organisation?
  - a. 0-150k
  - b. 151k-400k
  - c. 401k-1m
  - d. 1.1m-2m
  - e. 2.1m-3m
  - f. 3.1m-5m
  - g. 5m-10m
  - h. 10.1m-15m
  - i. 15.1m-50m
  - j. 51m or above
9. How many years has your organisation been in existence?  
 Years

**Information Security**

10. Which of the following information security controls does your organisation employ? (choose all applicable controls)

**Technical controls:**

- a. Hardware (e.g. firewall, IPS, etc.)
- b. Software (e.g. antivirus, configurations, etc.)

**Physical controls:**

- c. Personnel (e.g. security guard, CCTV, lock & key, etc.)

**Administrative controls:**

- d. Policy
- e. Security Education Training and Awareness (SETA) programs
- f. No information security
- g. Other (please specify):.....

11. Which of the following informs the selection of information security controls employed by your organisation? (choose all applicable)

- a. Past experiences (including personal experience)
- b. Information Security Best Practices and Standards (e.g. ISO27000 series, NIST SP800 series)
- c. Organisation Objectives
- d. Risk Assessment
- e. Observing Competitors
- f. Nothing/ implemented as needed
- g. Other (please specify) \_\_\_\_\_

12. In your opinion, how important are information security requirements in the development of an information security management system and the selection of information security controls?

- a. Not important at all
- b. Fairly important
- c. Moderately important
- d. Important
- e. Very important

13. Please motivate your answer to Question 12

Timothy Speckman 212455710

M. IT Research Survey

2017

14. How many qualified information security specialist, or the services thereof, does your organisation employ? (this includes information security consultants)
- a. 0
  - b. 1-2
  - c. 3-4
  - d. 5 or more (please specify):.....

15. According to your understanding, what are information security requirements?

16. What is your understanding of information security, pertaining to business information?

17. Choose all challenges which your organisation faces in implementing information security and give a few examples of how these challenges affect its implementation.
- a. Lack of financial resources



Timothy Speckman 212455710

M. IT Research Survey

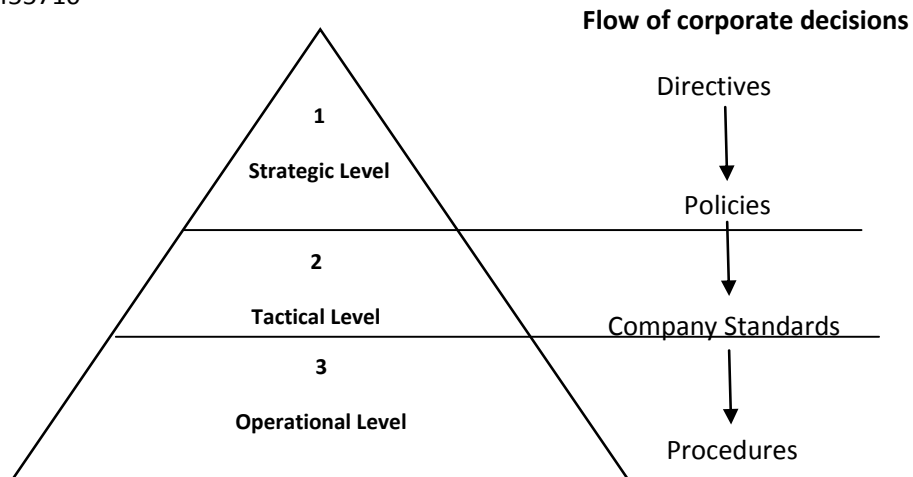
2017

- b. Lack of time
- c. Lack of expertise
- d. Lack of proper governance
- e. Other (please specify):.....

18. Please provide a few examples of how the challenges mentioned in Question 17, affect the implementation of information security.

**Information Security Governance**

19. According to your understanding, what do you perceive as information security governance?



**Figure 1: The Corporate Governance Model (adapted from von Solms & von Solms, 2009, pp. 3)**

20. Refer to Figure 1. Do layers 1, 2 & 3, of this model, resemble the management structure of your organisation?
- a. Yes
  - b. No
  - c. I do not know

21. Please elaborate on your answer to Question 18

22. Refer to Figure 1. Which of the management tiers take part in the governance of information security?
- a. Layers 1 & 2
  - b. Layers 2 & 3
  - c. Layers 1,2 & 3
  - d. Layers 1 & 3
  - e. I do not know
  - f. No information security governance
  - g. Other (please specify).....

23. Does your organisation make use of an Information Security Management System (ISMS), or any other system for reviewing, upgrading and improving the information security controls?
- a. Yes
  - b. No
  - c. I do not know

24. Please describe the system, or motivate your answer to Question 23.

25. Does your organisation have any other operative business process management system in place, such as a business continuity management system, a quality management system, or an environmental management system? Choose all that apply to your organisation.
- a. Business Continuity Management System
  - b. Quality Management System
  - c. Environmental Management System
  - d. I do not know
  - e. Other (please specify).....

26. Pertaining to the implementation of information security best practices in your organisation, e.g. ISO 27002, which of the following statements is most accurate? Information security best practices are...
- a. Easy to understand
  - b. Too complex for my organisation
  - c. Resource intensive
  - d. Other (please specify).....

27. Please motivate the answer you gave to question 26.

**Management Alignment**

28. To what extent are the information security controls, employed by your organisation, traceable back to higher management level decisions (as depicted by the flow of corporate decisions in figure 1), showing alignment throughout the enterprise?

- a. Not at all
- b. Visible relationship
- c. Fairly traceable
- d. Fully traceable
- e. I do not know

29. Please motivate the answer you gave to question 28.

30. In your opinion, how important is it for the information security requirements at each management level, to relate to a directive/decision from a higher management level (as depicted by the flow of corporate decisions in Figure 1)?

- a. Not important at all
- b. Fairly important
- c. Moderately important
- d. Important
- e. Very important

31. Please motivate the answer you gave to question 30.

32. How easy is it for you to establish the information security requirements of the enterprise, while ensuring that they align at each of the management levels? (e.g. incorporating enterprise objectives from strategic level management, into the Corporate Information Security Policy at the tactical level management, as depicted in Figure 1)

- a. Very hard
- b. Hard
- c. Moderate
- d. Easy
- e. Very easy

33. Please motivate the answer you gave to question 32.

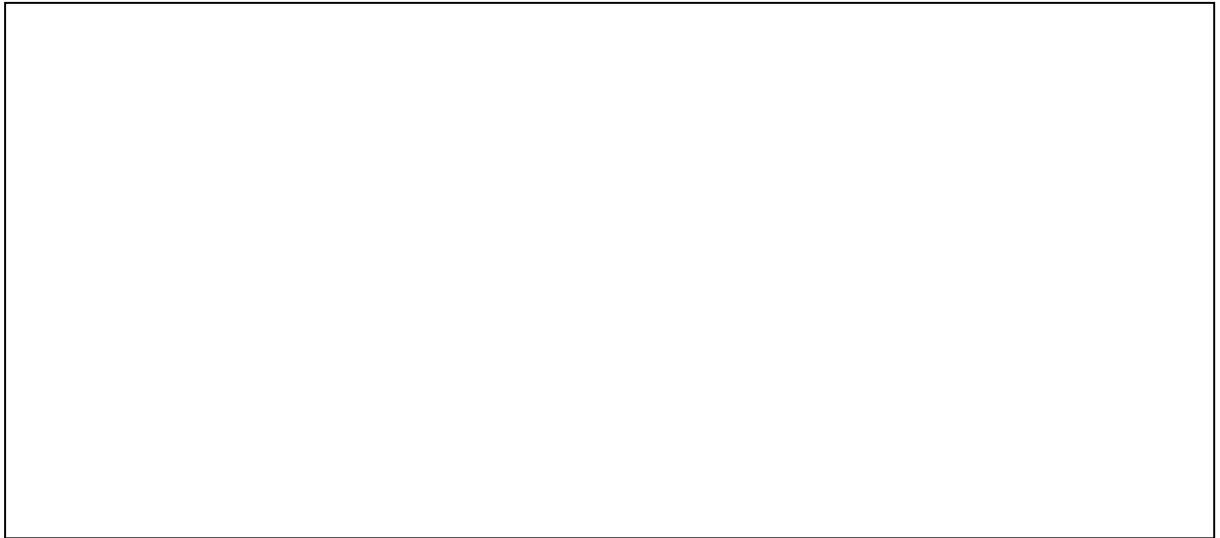
34. Do you think that a model, which provides guidance on establishing information security requirements at each of the management levels of an organisation and is simplified to meet the needs of SMMEs; would be of assistance in developing the information security management system of your organisation?

- a. Yes
- b. No
- c. I do not know

35. Please elaborate on the answer you gave to question 34.

Timothy Speckman 212455710  
M. IT Research Survey  
2017

36. Please make a few suggestions that the designer of a model for SMMEs should consider, in order for it to be feasible for SMMEs to make use of such a model.

A large, empty rectangular box with a thin black border, intended for the respondent to provide suggestions for model designers.

# Appendix C

## The Information Security Expert Interview

As reported in Chapter 8, an information security expert was interviewed for the evaluation of the MAISRSS. Before evaluating the model, the information security expert was furnished with a suite of documents, which include:

1. A Cover Letter (C.1)
2. Background Information (C.2)
3. Definition of Information Security Requirements (C.3)
4. Draft Principles for Developing the MAISRSS (C.4)
5. The Expert Interview Questionnaire (C.5)

A short video demonstration of the automated tool was also sent to the information security expert and can be found on the compact disc attached to this dissertation. The title of the video is "TH Speckman Information Security Expert Interview 2018". VLC is the recommended player to use when viewing the video.

## **C.1 Information Security Expert Interview: Cover Letter**

The following is an example of the cover letter that was sent to the information security expert during the evaluation of the MAISRSS.



Good day...,

Thank you for taking time from your busy schedule, to participate in this research study. Your time and input are highly appreciated. We understand that time is a scarce commodity for a highly sought individual, such as yourself.

To simplify the process, while providing enough information to evaluate the model, the supplied components are as follows:

1. A short video with background information, giving an overview of the research study.
2. Secondly, appendices are attached with further information to be read if required. This information is found in:
  - a. Appendix A: Background information
  - b. Appendix B: Information security requirements
  - c. Appendix C: Deriving the draft principles
3. The expert interview, in the form of a questionnaire.

The model developed in this research study (Model for the Alignment of Information Security Requirements within South African SMMEs (MAISRSS)), is part of my master's research project. This research project is completed under the supervision of Professor Mariana Gerber, at the Nelson Mandela University.

Your feedback from the evaluation of the MAISRSS, will be used improve the model where necessary. Only the completed questionnaire is required to be returned to the researcher via email. The questionnaire consists of 25 questions, which can be completed in 20 to 40 minutes.

I do understand that time does not always lend itself to such matters; however as time constraints put pressure on most research studies, please do complete and return the questionnaire to the researcher by Friday the 15<sup>th</sup> of June 2018.

Please do not hesitate to contact the researcher if any further information is required. Once again, I thank you for your time.

Kind regards,

Timothy Speckman.

[S212455710@mandela.ac.za](mailto:S212455710@mandela.ac.za)

Cell: 078 773 1195

## **C.2 Information Security Expert Interview: Background Information**

The suite of information sent to the information security expert included background information, as can be seen below. The background included information about the context of the research project and the identified problem.

## **Appendix A: Background Information**

### **A Model for the Alignment of Information Security Requirements within South African SMMEs**

According to Smit and Watkins (2012), most South African (SA) small medium and micro enterprises (SMMEs), implement information security controls on an ad-hoc basis mostly in reaction to an information security incident. Furthermore, the ad-hoc implementation of information security controls, results in the implementation of unnecessary information security controls and the over-management of information security risks. Thus, Smit and Watkins, suggest that SA SMMEs should implement an information security risk management approach that is integrated into the corporate governance structure of the organisation. Additionally, this information security risk management approach should prevent the over-management of information security risks within these organisations.

An information security management system (ISMS), presents a comprehensive and efficient manner in which to manage the information security efforts of an organisation. More so, the development of an ISMS involves the executive management of an organisation and is therefore part of the corporate governance of an organisation (Calder, 2009, p 3). Thus, an ISMS is based on the unique information security requirements of an organisation (ISO/IEC27001, 2013, p v). The information security requirements of an organisation are established by conducting an information security requirements analysis, as reported in ISO/IEC27003 (2010). However, Van Niekerk and Labuschagne (2006), report that most well-known information security best practices and standards, such as the ISO/IEC27000 family, are too complex and resource intensive for SMMEs to implement.

Therefore, this research study was conducted to develop a simpler method for SA SMMEs to establish their unique information security requirements. The researcher therefore set out to discover four factors that could influence the design and development of this simpler method. Firstly, to understand the perspective of various literature on the use of information security requirements and what they are (*perspective*). Secondly, the definition of information security requirements, from information security best practices and standards (*criteria*). Thirdly, the core elements of an artefact developed for SMMEs (*core elements*). Fourth and finally, the researcher established what the outcomes of effective information security governance are (*outcomes*), to ensure that the developed method will contribute to effective information security governance.

Upon discovering the perspective, criteria, core elements and outcomes, a survey was conducted. The purpose of the survey was to confirm the existence of the phenomena discovered through the literature survey, in an SA SMME context. Through the few responses received from the survey, the phenomena appeared to exist in the SA SMME context too. Therefore, the perspective, criteria, core elements and outcomes were used to derive seven draft principles. These draft principles are required by the research design that was used to conduct the research study, design-based research (Herrington, McKenney, Reeves, & Oliver, 2007).

The seven draft principles, as seen below, guided the design and development of the model, as the simpler method, output by this research study:

1. **Strategic alignment**- to ensure that the information security efforts of the organisation are aligned with the business strategy, principles and objectives for information security governance.
2. **Risk control**- clearly showing how information security risk management decisions are made within the organisation, giving executive level management an insight on these decisions.
3. **Feasibility**- making the model implementable even under the limited financial resources, human resources and expertise of SMMEs.
4. **Performance measurement**- using information security requirements as a metric to measure the effectiveness of the implemented information security controls of an organisation.
5. **Utility**- in preventing the over-management of information security risks, the model should allow for the optimisation of information security investment according to the size and level of maturity of the organisation.
6. **Simplicity**- the processes of the model to determine information security requirements, should be easily integrated with the business processes of the organisation rather than using information security best practices and standards.
7. **Due diligence**- the model should depict how an organisation took reasonable steps to establish and understand its information security requirements and what decisions were taken regarding its established information security requirements.

As discussed above, these draft principles were used to guide the design and development of a model known as the Model for the Alignment of Information Security Requirements within SA SMMEs (MAISRSS). The MAISRSS, is proposed as a simpler method for SA SMMEs to establish the unique information security requirements of the organisation that are aligned with the business strategy, principles, objectives and business requirements for information processing. Seen in Figure 1, below, is the MAISRSS.

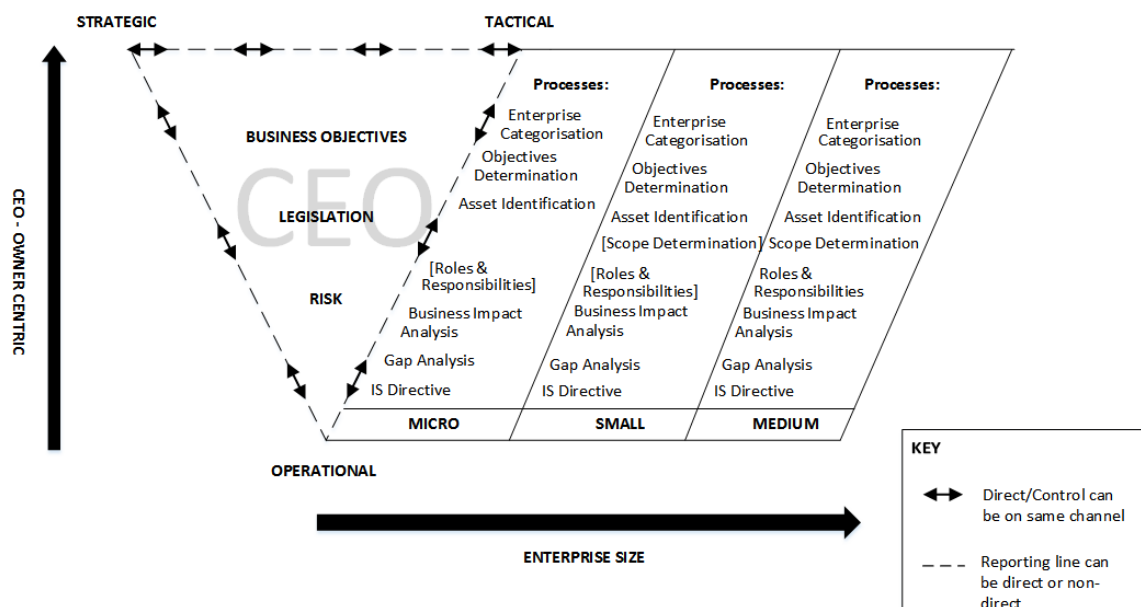


Figure 1: The Model for the Alignment of Information Security Requirements within SA SMMEs (MAISRSS)

As seen in Figure 1, above, the MAISRSS is structured in such a manner that it is representative of both the flexible and informal, CEO-owner centric corporate governance management structure reported by Hankinson, Bartlett and Ducheneaut (1997); and the SMME organisational structure described by Beaver and Prince (2004). Thus, the MAISRSS provides utility for the organisation even as it grows in size and matures in its business processes.

The processes of the MAISRSS, are based on guidance for the development of an ISMS as seen in ISO/IEC27001 (2013) and ISO/IEC27003 (2010) and the information security risk management standard (ISO/IEC27005, 2011). These processes are optional (indicated by means of square braces [ ]) for some categories of SMMEs, while mandatory for others and are influenced by the draft principles as discussed below:

1. **Enterprise categorisation-** Calder (2009, p 36), claims that the scope of an ISMS depends on the size of the organisation, with smaller organisations including everything in the scope of the ISMS. Likewise, the information security requirements will be determined for the information assets within the scope of the ISMS. Additionally, to provide utility it is necessary to support the scalability of the rapidly evolving SMMEs. For this reason, the category of SMME is established according to criteria in the National Small Business Act of 1996, in order to categorise an organisation as micro, small or medium.
2. **Objectives determination-** compulsory to all categories of SMMEs, supports the draft principle of strategic alignment by assisting organisations to determine their information security objectives and principles.
3. **Asset identification-** is a process with the objectives of identifying information assets within the scope of the ISMS, which an organisation must protect. Thereby addressing the risk control, due diligence and simplicity draft principles.
4. **Scope determination-** addresses the draft principles of utility, feasibility and simplicity by ensuring that the scope of the ISMS includes only what is necessary to meet its information security objectives and principles.
5. **Roles and responsibilities-** concerning the protection of information assets are assigned to individuals or departments with the organisation. Thus, this process addresses the feasibility, risk control and utility draft principles.
6. **Business impact analysis-** is a process to measure the potential impact that a success information security threat could have on the organisation and its operations. This process is related to the draft principles risk control, due diligence and utility.
7. **Gap analysis-** is a process performed to determine whether or not the organisation has met its information security objectives and principles. This process also determines whether current information security efforts are effective in protecting the information assets of the organisation. Therefore, this process relates to risk control, performance measurement, due diligence, utility and strategic alignment.
8. **IS directive –** is the final process and the one in which the information security requirements and the intent to fulfil these information security requirements is communicated by the executive management of the organisation. This process addresses all of the draft principles, as a high level information security policy is generated and details the outcomes of the previous processes, which addressed the draft principles as discussed above. The output of this process is a policy document with the level of information security required for the identified information assets of the organisation and how these information security

requirements will be met. For further reading on information security requirements, see Appendix B.

## References

- Beaver, G., & Prince, C. (2004). Management, strategy and policy in the UK small business sector: a critical review. *Journal of Small Business and Enterprise Development*, 11(1), 34–49. <https://doi.org/10.1108/14626000410519083>
- Calder, A. (2009). *A Management Guide: Implementing Information Security based on ISO 27001/ ISO 27002*. (J. van Bon & S. Polter, Eds.). Van Haren Publishing.
- Hankinson, A., Bartlett, D., & Ducheneaut, B. (1997). The key factors in the small profiles of small-medium enterprise owner-managers that influence business performance: The UK (Rennes) SME survey 1995-1997 An international research project UK survey. *International Journal of Entrepreneurial Behavior & Research*, 3(3), 168–175.
- Herrington, J., McKenney, S., Reeves, T. C., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In *World Conference on Educational Multimedia, Hypermedia and Telecommunications* (pp. 4089–4097). Chesapeake, VA. Retrieved from <http://ro.ecu.edu.au/ecuworks/1612>
- ISO/IEC. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.
- ISO/IEC27003. (2010). *Information technology — Security techniques — Information security management system implementation guidance*. Geneva.
- ISO/IEC27005. (2011). *Information technology — Security techniques — Information security risk management*. Geneva.
- Smit, Y., & Watkins, J. A. (2012). A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African Journal of Business Management*, 6(21), 6324–6330. <https://doi.org/10.5897/AJBM11.2709>
- Van Niekerk, L., & Labuschagne, L. (2006). The PECULIUM model: information security risk management for the south african SMME.

### **C.3 Information Security Expert Interview: Information Security Requirements Definition**

To avoid confusion and to assist the information security expert in further understanding the research project, a detailed discussion on information security requirements was also included in the suite of documents and can be seen below.

## **Appendix B: Information Security Requirements**

Organisations, implement information security in an attempt to make their information secure against malicious attacks (Calder, 2009, p 19). However information security solutions implemented by organisations are often designed, acquired and implemented on a tactical basis, to meet a specific situation. This often results in a multitude of technical solutions, each independently designed, with no consideration of the strategic dimension or the goals of the business (Sherwood, 1996). Although information security management standards such as ISO 27002 exists to assist organisations in developing and implementing information security, the adoption of these standards is not a straight forward process for any organisation, let alone an SMME (Barlette & Fomin, 2008). Tailoring information security best practices and standards to the information security requirements of an organisation could result in a business-driven information security architecture, which describes a structured inter-relationship between the technical and procedural solutions to support the long-term business needs of the organisation (ITGI & OGC, 2008, p 6).

This paper describes a model developed to assist South African (SA) small, micro and medium organisations (SMMEs) in tailoring information security best practices and standards to their information security requirements. The model was developed with the varying management structures of SMMEs in mind and the low resources found in these organisations. In presenting the need for the model, this paper begins with a discussion of information, corporate governance, the corporate governance of information and communication technology and information security governance, This paper further goes on, to discuss what information security requirements are, what SMMEs are, particularly in an SA context, as well as their management structures. The research methodology used for this study will also be mentioned, before the proposed model is introduced.

### **II. INFORMATION SECURITY GOVERNANCE**

Before defining and discussing information security governance, it is necessary to understand what information, corporate governance and the corporate governance of information and communication technology are. Therefore this section discusses these concepts in that order.

#### **A. Information**

Computers and the use thereof have evolved rapidly over time. More importantly their role and use in organisations has also evolved greatly, due to benefits provided by information and communication technology (ICT) such as competitive advantage and timely access to information among others. This evolution has brought about great change, with a shift from the computer-centric era where the physical protection of the ICT infrastructure was the main concern, to an information-centric era, where information is reported to be the life-blood of an organisation (Gerber & Solms, 2001; Vermeulen & Von Solms, 2002).



In the information-centric era, useful data, known as information is reported to be one of the most critical strategic assets of an organisation. Failure to adequately protect the information assets of an organisation could result in calamitous risks, even including the demise of an organisation. Therefore, the protection of this information and its related technology is reported to form part of the corporate governance responsibility of an organisation (ISO/IEC27002, 2013, p viii; Whitman & Mattord, 2012; IoDSA, 2009; von Solms & von Solms, 2009, p 19).

## B. Corporate Governance

Corporate governance is the relationship between the various participants involved in determining the direction and ensuring the performance and well-being of an organisation, also referred to as the system by which the organisation is directed and controlled (Monks & Minow, 2004; IoDSA, 2009, p 6; OECD, 2015, p 11; von Solms & von Solms, 2009, p 1; ISO/IEC38500, 2008, p 3 ). The participants of corporate governance can be grouped into three main levels of management, namely: strategic-level management (board of directors and executive management, who provide the organisation with direction in the form of directives); tactical-level management (middle-level management, who translate the directives received from strategic management and implement them as policies, procedures and company standards); and operational-level management (lower-level management, responsible for ensuring the implementation of the policies, procedures and company standards in the day to day operations of an organisation) (von Solms & von Solms, 2009, p 3). Corporate governance is concerned with the performance and well-being of an organisation; thus it is imperative that the well-being of assets which are critical to the survival of the organisation and related technology (ICT) form part of the corporate governance structure.

## C. Information and Communication Technology Governance

ICT governance is a component of corporate governance and is the structure through which management of an organisation attempts to ensure that the organisation's ICT investment is strategically aligned with the objectives of the organisation and is used in a manner that mitigates the associated risks (ISO/IEC38500, 2008, p 3; von Solms & von Solms, 2009, p 10; Ayat M., Masrom M., & Sahibuddin S., 2011; Devos, Van Landeghem, & Deschoolmeester, 2012).

However the security achieved purely through technical means and by only addressing risks to the ICT is limited, as it often only addresses the security needs of the hardware and infrastructure and not those of the information. Business or personal information needs to be protected wherever it resides (ISO27002, 2012, p. viii; Gerber, von Solms & Overbeek, 2001).

#### D. Information Security

Therefore it is necessary to protect the information from inadvertent or malicious changes, deletions or unauthorised disclosure. This is known as information security and in full is defined as “all the aspects related to achieving and maintaining confidentiality, integrity, availability, accountability, authenticity and reliability” (Gerber, Von Solms, & Overbeek, 2001).

Information security is such an important aspect of an organisation that it should be addressed at an executive management level (Posthumus & von Solms, 2004).

#### E. Information Security Governance

The process of governing information security at an executive level is known as information security governance (Posthumus & von Solms, 2004).

However it has been reported that many organisations design and install information security solutions on a tactical basis. This results in a build-up of a mixture of technical solutions on an ad-hoc basis. These independently developed solutions have no guarantee that they will be compatible and interoperable or even worse that they can support the goals of the business (Sherwood, 1996).

“The solution would be the development of an organisation security architecture, which is business driven and describes a structured inter-relationship between the technical and procedural solutions, to support the long-term business needs of the organisation. This requires a thorough understanding of the information security requirements of the organisation” (Sherwood, 1996).

### III. INFORMATION SECURITY REQUIREMENTS

Information security requirements can be defined as “the amount of security needed to provide the required level of information security.” This can be interpreted as the security concerns of the organisation, combined with the level of security required for each concern, resulting in the information security requirements (Gerber & Solms, 2001).

Information security requirements provide management with a starting point in the development of an organisation-wide information security strategy. These information security requirements stem from three main sources, being:

- Firstly, by assessing the risk to the information assets of an organisation;
- Secondly, the legal, statutory, regulatory and contractual requirements to be fulfilled by the organisation, its contractors, trading partners and service providers and;

- Thirdly, the set of principles, objectives and requirements for information handling, processing, storing, communicating and archiving that an organisation has developed to support its operations (ISO/IEC27002, 2013, p v; Gerber & Solms, 2001).
- Information security requirements feature at different levels of management within an organisation. The detail of the information security requirements varies according to the level of management. The information security requirements are communicated via the inter-tier and intra-tier communications, in the same way that business directives are communicated through the organisation management structure (NISTSP800-53, 2013, p 8).

With reports of information security solutions being designed, acquired and implemented on an ad-hoc basis, there is an indication of misalignment or lack of communication of the strategic directives and the rest of the organisation (Sherwood, 1996; D'arcy, Herath, & Shoss, 2014).

Unclear information security requirements can often lead to coping methods such as non-compliance. This non-compliance can be implementation of technology and solutions on an ad-hoc basis, just to get the job done or a complete disregard of tasks set out to fulfill the information security requirements (D'Arcy, Herath, & Shoss, 2014).

Although information security best practices and standards exist to assist organisations in the development of an organisation information security architecture they are reported to be resource intensive and complex to implement if treated purely as technical guidance (Van Niekerk & Labuschagne, 2006). Therefore management and staff must understand what to do, how to do it and why it is important. This task is often daunting for organisations without the proper know-how or expertise to understand and implement these best practices and standards (ITGI & OGC, 2008, p 6).

## References

- Barlette, Y., & Fomin, V. V. (2008). Exploring the suitability of IS security management standards for SMEs. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. <https://doi.org/10.1109/HICSS.2008.167>
- Calder, A. (2009). *A Management Guide: Implementing Information Security based on ISO 27001/ ISO 27002*. (J. van Bon & S. Polter, Eds.). Van Haren Publishing.
- D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318. <https://doi.org/10.2753/MIS0742-1222310210>
- Gerber, M., & Solms, R. Von. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, 20, 577–584.
- Gerber, M., Von Solms, R., & Overbeek, P. (2001). Information Management & Computer

Security Formalizing information security requirements. *Information Management & Computer Security Iss Information Management Computer Security Iss Industrial Management & Data Systems Iss Information Management & Computer Security Iss*, 9(17), 32–37. Retrieved from <http://dx.doi.org/10.1108/09685220110366768>

Iso/lec. (2008). SANS 38500 : 2009 SOUTH AFRICAN NATIONAL STANDARD Corporate governance of information technology. *Sans 38500:2009*, 1–25.

Iso/lec27002. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

ITGI, & OGC. (2008). *Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit\_res\_Eng\_1108*.

Monks, R., & Minow, N. (2004). *Corporate Governance*. Malden, MA: Blackwell Publishing.

NISTSP800-53. Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations (2013).

Posthumus, S., & von Solms, R. (n.d.). A framework for the governance of information security. <https://doi.org/10.1016/j.cose.2004.10.006>

Sherwood, J. (1996). SALSA: A Method for Developing the Enterprise Security Architecture and Strategy. *Computers & Security*, 15, 501–506.

Van Niekerk, L., & Labuschagne, L. (2006). The PECULIUM model: information security risk management for the south african SMME.

Von Solms, R., & (Basie) von Solms, S. H. (2009). *Information Security Governance*. New York: Springer Science. <https://doi.org/10.1007/978-0-387-79984-1>

## **C.4 Information Security Expert Interview: Draft Principles**

The information security expert was then informed about the draft principles that guided the development of the MAISRSS and how the draft principles were derived. Below is the discussion of the draft principles, which was presented to the information security expert.

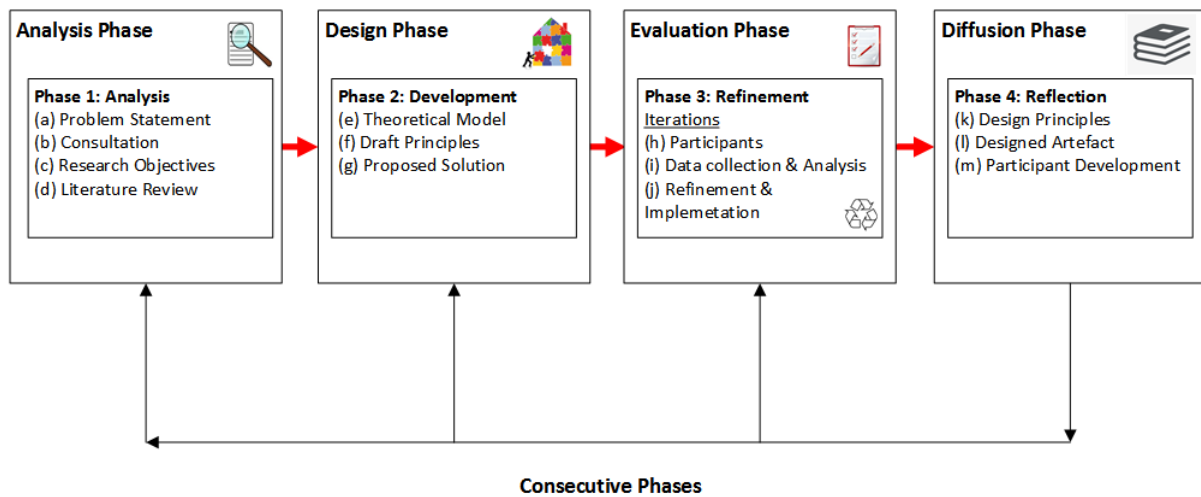
## **Appendix C: Deriving the draft principles**

This document briefly explains how the researcher concluded on the seven draft principles as seen in Appendix A: Background.

Throughout this research study, a four phased unique integrated research design was followed. This research design was a unique integration of design-oriented IS research by Osterle et al., (2010) and Herrington, McKenney, Reeves and Oliver (2007). The unique integrated research design consists of four phases as seen in Figure 1. These four phases are:

1. The **Analysis Phase** is the first phase of the integrated research design. As seen in Figure 1 below, the tasks for this phase are problem statement, consulting researchers and practitioners, research objectives and literature review.
2. The second phase of the integrated research design is known as the **Design Phase**. According to this phase, researchers are required to complete three tasks. Firstly, theoretical model based on literature must be constructed. Secondly, draft principles must be derived to guide the design of the proposed solution. Thirdly, the researcher should provide a description of the proposed solution.
3. In the unique integrated research design, the **Evaluation Phase** is the third phase of the four phased research design. The tasks to be completed in the Evaluation Phase of the integrated research design are identifying practitioners as participants for the evaluation process. Secondly, the researcher is required to collect data related to the perception and opinion of practitioners pertaining to the proposed model. The third task involves making the necessary refinements to the solution, as established through the analysis of data collected from practitioners.
4. Finally, in the **Diffusion Phase** of the unique integrated research design, the research distributes of the findings of the research study by publishing design principles to guide the implementation of the solution, the designed artefact and professionally developing participants of the research study.

## Integrated Research Design



**Figure 1: Unique integrate research design**

Therefore according to the Design Phase of the unique integrated research design, the researcher to derived draft principles. The purpose of the draft principles was to guide the design and development of the proposed model as the artefact output by this research study (Herrington et al., 2007).

As recommended by Herrington et al. (2007), the draft principles are based on existing knowledge, as seen in Table 1 below.

<b>Outcomes of Effective IS Governance (G)</b>	<b>SMME Artefact Core Elements (E)</b>	<b>IS Requirements Perspective (P)</b>	<b>IS Requirements Criteria (C)</b>
1. Strategic alignment	1. Scalability	1. IS measurement	1. Source 1
2. Risk management	2. Simplicity	2. Identify appropriate IS controls	2. Source 2
3. Resource management	3. Feasibility	3. Suit different organisation sizes	3. Source 3
4. Performance measurement	4. Utility		
5. Value delivery	5. Transparency		
6. Business process convergence	6. Risk control		

**Table 1: Findings from the literature review**

As mentioned above, Herrington et al. (2007), recommend that the draft principles to guide the design and development of the artefact should be based on existing knowledge. Thus each of the columns in Table 1 is populated with findings from a literature review.

The labels in brackets in each of the draft principles show a link between the draft principle and the column in Table 1. Column (C) of Table 1 refers to the three sources of information security requirements, as seen in Appendix B.

Although named draft principles, these should not be confused as a preliminary version of the principles. The term draft in this context refers to the use of the principles to guide the design and development (the draft) of the proposed model. The seven draft principles derived to guide the design and development of the proposed model:

1. **Strategic alignment**- an organisation should exhibit transparency (*E5*) on how strategic decisions, taking by executive management of the organisation regarding IS governance, get translated to information security controls and roles and responsibilities. Therefore, the information security efforts of an organisation should be aligned with the business strategy, principles, and business requirements of the organisation for information processing (*C2*). In doing so, the information security efforts of the organisation will support the organisational objectives of the organisation (*G1*).
2. **Risk control**- it must be clear how decisions are made within an organisation, to assess the risk to its information assets (*C1*) and how appropriate information security controls are selected to address this risk (*G2, P2*). Thereby, enabling the executive management of the organisation to have insight on the decisions taken regarding IS risk management (*E6*).
3. **Feasibility**- due to the limited human resources, limited finance, limited expertise and poor infrastructure (*E3*), the proposed model should not be resource intensive. Furthermore, where available the information security knowledge and infrastructure of the organisation should be utilised efficiently and effectively (*G3*).
4. **Performance measurement**- IS requirements should be used as a metric to measure the effectiveness of information security efforts (*P1*) in achieving the information processing and IS objectives of the organisation (*G4*).
5. **Utility**- the proposed must be fit for purpose (*E5*) in optimising the information security investment of an organisation, according to the size and level of maturity of the organisation (*P3*), to support its organisational objectives (*G5*).
6. **Simplicity**- the processes of the proposed model, must be easily integrated with the processes of an organisation (*G6*), without hindering the ability of SMMEs to quickly respond to customer demands (*E2*).
7. **Due diligence**- an organisation, which has implemented the proposed model should be able to show that due diligence was done. For this reason, organisations should show that reasonable steps were taken to ensure to avoid contravention of legal, statutory, regulatory and contractual requirements (*C3*).



## References

- Herrington, J., McKenney, S., Reeves, T. C., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In *World Conference on Educational Multimedia, Hypermedia and Telecommunications* (pp. 4089–4097). Chesapeake, VA. Retrieved from <http://ro.ecu.edu.au/ecuworks/1612>
- Osterle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., ... Sinz, E. J. (2010). Memorandum on design-oriented information systems research. *European Journal of Information Systems*, (October), 1–4. <https://doi.org/10.1057/ejis.2010.55>

## **C.5 Information Security Expert Interview: Questionnaire**

Finally, the information security expert was asked to evaluate the extent to, which the MAISRSS conforms to the draft principles. The questionnaire that was used for the evaluation, can be seen below.

# A Model for the Alignment of Information Security Requirements within SA SMMEs

Expert Interview Questionnaire

May 2018

## Background Information

*This section of the questionnaire pertains to information relating to the qualifications and experience of the information security expert evaluating the model, in this area of research.*

Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box.

1. Please provide your name, surname and title (e.g. Mr, Miss, Mrs, Dr, Prof., etc.).

Name	Surname	Title

2. What is your current occupation and job title/description?

Occupation	Job Title/Description

3. Please rate the extent to which the qualification you possess, is relates to information security or information security governance.

Strongly related	Related	I am not sure	Somewhat related	Completely unrelated
------------------	---------	---------------	------------------	----------------------

4. How many years of experience do you have in the information security or information security governance field?

years.

5. Based on your experience and knowledge, to what extent would you agree that you are confident in answering questions related to information security and/or information security governance?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

6. Please rate the extent to which you have experience in working with information security governance in SMMEs.

Highly experienced	Experienced	I am not sure	Somewhat experienced	Completely inexperienced
--------------------	-------------	---------------	----------------------	--------------------------

7. How frequent has your experience involved working with information security or information security governance in SMMEs?

Very frequently	Frequently	Occasionally	Rarely	Never
-----------------	------------	--------------	--------	-------

8. Based on your knowledge and experience of working with SMMEs, to what extent do you rate yourself as confident in answering questions related to information security governance in SA SMMEs?

Very confident	Confident	Neutral	Not so confident	Not confident at all
----------------	-----------	---------	------------------	----------------------

9. Based on your knowledge and experience of information security and or information security governance, please indicate the extent to which you rate yourself as confident to answer questions related to information security management systems (ISMS)?

Very confident	Confident	Neutral	Not so confident	Not confident at all
----------------	-----------	---------	------------------	----------------------

10. Please indicate the extent to which you are confident in your knowledge and ability to answer questions related to information security requirements.

Very confident	Confident	Neutral	Not so confident	Not confident at all
----------------	-----------	---------	------------------	----------------------

### General Principles

*Refer to Appendix A: Background information to answer questions 11 to 17. The general principles section attempts to establish the understanding and opinion of the expert evaluating the model, pertaining to the research problem to be solved by this research study.*

Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box.

11. Please indicate the extent to which you agree that an ISMS is the most comprehensive approach for an organisation to manage its information security efforts.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

12. Based on your knowledge and experience, how often is your answer to the previous question true for SA SMMEs too?

Almost always true	Usually true	Occasionally true	Usually not true	Almost never true
--------------------	--------------	-------------------	------------------	-------------------

13. Please elaborate on your answer to Question 12.

--

14. In your knowledge and experience, how true is it that the development of an ISMS and the selection of information security controls should be based on the unique information security requirements of an organisation?

Almost always true	Usually true	Occasionally true	Usually not true	Almost never true
--------------------	--------------	-------------------	------------------	-------------------

15. Please indicate how often you think it is true that SMMEs have unique characteristics and constraints that make them different to larger organisations?

Almost always true	Usually true	Occasionally true	Usually not true	Almost never true
--------------------	--------------	-------------------	------------------	-------------------

16. Based on your knowledge and experience, how often does the corporate governance structure within SMMEs appear to be more CEO or owner centric (flat structure), compared to the three tiered management structure of large organisations?

Very frequently	Frequently	Occasionally	Rarely	Never
-----------------	------------	--------------	--------	-------

17. To what extent do you agree that the characteristics and constraints of SMMEs often presents a challenge when attempting to implement information security standards and best practices such as ISO/IEC27001?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

### Draft Principles

*This section of the questionnaire attempts to assess the extent to which the developed model, adheres to the draft principles which guided its design and development.*

Refer to the Appendix A: Background Information and Appendix C: Draft Principles, to answer the questions that follow. Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box.

18. To what extent do you agree that the model in Appendix A, is representative of the flat structure of the corporate governance management structure of most SA SMMEs?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

19. Please indicate the extent to which you agree that the processes and the management structure depicted by the model promote strategic alignment, by showing how executive level management decisions regarding information security governance, are translated into information security requirements.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

20. To what extent would you agree that the output of the processes depicted in the model will allow the executive level management of an organisation to have an insight about decisions that are made regarding information security risk management?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

21. Based on your knowledge and experience, to what extent do you agree that the processes depicted in the model present a method simplified for SA SMMEs to establish their unique information security requirements, while being feasible enough to implement where human resources, finance and information security expertise are limited?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

22. Indicate the extent to which you agree that the information security requirements established through the processes of the model will be sufficient metrics for SA SMMEs to measure the performance of current and future information security efforts.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

23. To what extent do you agree or disagree that the corporate governance management structure and processes of the model will remain applicable in determining the information security requirements and optimising the information security investments of an SMME, even as it matures?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

24. Based on your knowledge and experience, to what extent do you agree that the processes depicted in the model are simple enough for an SA SMME to implement without disrupting its business operations?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

25. Based on your knowledge and experience of information security governance, how true would you say it is that the executive level management of an organisation can claim that due diligence was done with regards to information security, by performing the processes depicted in the model?

Almost always true	Usually true	Occasionally true	Usually not true	Almost never true
--------------------	--------------	-------------------	------------------	-------------------

26. Please provide any suggestions, recommendations or opinions that could assist the researcher in improving the model.

**Thank you for your time and invaluable participation.**

# Appendix D

## The SMME Expert Interview

An SMME expert was interviewed for the evaluation of the automated tool that was developed based on the MAISRSS. Similar to the information security expert interview, the SMME expert was furnished with a suite of documents, as follows:

1. A Cover Letter (D.1)
2. Background Information (D.2)
3. Expert Interview Questionnaire (D.3)

A short video demonstration of the automated tool was also sent to the SMME expert and can be found on the compact disc attached to this dissertation. The title of the video is "TH Speckman Automated Tool Demonstration Video".

## **D.1 SMME Expert Interview: Cover Letter**

The cover letter that was sent to the SMME expert, seeking his/her participation in evaluating the automated tool, can be seen below.



August 2018

Good day Sir/Madam,

Thank you for taking time from your busy schedule, to participate in this research study. Your time and input are highly appreciated. We understand that time is a scarce commodity for a highly sought individual, such as yourself.

To simplify the process, while providing enough information to evaluate the model, the supplied components are as follows:

1. A short video demonstration, giving an overview of the tool.
2. Secondly, an appendix is attached with further information to be read if required. This information is found in:
  - a. Appendix A- Research Field Background
3. The survey, in the form of a questionnaire.

The model developed in this research study (Model for the Alignment of Information Security Requirements within South African SMMEs (MAISRSS)) and the tool developed as a prototype, is part of my master's research project. This research project is completed under the supervision of Professor Mariana Gerber, at the Nelson Mandela University.

Your feedback will be used to improve the automated tool where necessary. Only the completed questionnaire is required to be returned to the researcher via email. The questionnaire consists of 20 questions, which can be completed in approximately 30 minutes.

I do understand that time does not always lend itself to such matters; however as time constraints put pressure on most research studies, please do complete and return the questionnaire to the researcher by Friday the 24<sup>th</sup> of September 2018.

Please do not hesitate to contact the researcher if any further information is required. Once again, I thank you for your time.

Kind regards,

Timothy Speckman.

s212455710@mandela.ac.za

Cell: 078 773 1195

## **D.2 SMME Expert Interview: Background Information**

The background information presented to the SMME expert was simpler than that presented to the information security expert. The researcher considered that the SMME expert had no expertise in the information security field. Therefore, only information necessary to understand the context of the research study was presented, as can be seen below.

## **Appendix A: Background Information**

### **A Model for the Alignment of Information Security Requirements within South African SMMEs**

It has been said that for most modern organisations to continue their business operations, they rely on information. Information can be defined as all data of useful meaning to an organisation. This data can be in the form of paper records, electronic media or intellectual property in people's heads (Brotby, 2009, p. 7; DTI, 2006, p. 3). Most organisations (including SMMEs) use information technology (IT) on a daily basis, to create, acquire, modify, store and transmit information. Therefore these IT systems and the information that they house, are reported to be valuable information assets of an organisation (Posthumus, von Solms, & King, 2010). The importance of information assets to an organisation being able to continue its business operations, warrants an investment in the protection of the information assets of an organisation (Whitman & Mattord, 2012, p. 11).

This document gives a brief background synopsis of the research area of this study. The components that make up the research area will briefly be discussed. These components are (in their order of discussion) information security and information security requirements. Furthermore, the model and automated tool that were developed from the findings of this research study.

#### **Information Security**

Information security has been defined as the protection of the significant characteristics of information assets. There are several significant characteristics of information assets; however confidentiality, integrity and availability are reported to be the three most critical ones. **Confidentiality** refers to the significant characteristic of information assets only being accessible to authorised users. **Integrity** refers to the information asset being altered or modified only by those who are authorised to do so in an authorised and desirable manner. **Availability** as a significant characteristic is concerned with authorised users being able to access the relevant information assets in the required format, without interference or obstruction, when needed (Whitman & Mattord, 2012, p. 6).

The significant characteristics of information assets are protected by implementing information security controls. Information security controls include policies, firewalls, antiviruses and others that safe guard the significant characteristics of information assets from information security threats (Whitman & Mattord, 2012, p. 8). Information security threats are undesirable events that may result in a loss of one or more significant characteristics of an information asset and possibly have an adverse effect on the business operations of an organisation (Peltier, 2004, p. 18).

Due to resource constraints such as a lack of expertise and finances, most South African (SA) small medium and micro enterprises (SMMEs), implement information security controls on an ad-hoc basis mostly in reaction to a successful information security threat. The ad-hoc implementation of information security controls, results in the implementation of unnecessary information security controls and the over-management of risks that an information security threat may be successful (Yolande Smit, 2012).

Therefore, SA SMMEs should implement information security controls that are based on the unique information security requirements of the enterprise (ISO/IEC27001, 2013, p. v).

## Information Security Requirements

Information security requirements can be defined as “the amount of security needed to provide the required level of information security.” This can be interpreted as the security concerns of the organisation (significant characteristics), combined with the level of security required for each concern, resulting in the information security requirements (Gerber & Solms, 2001).

Information security requirements provide the executive management of an organisation, with a starting point in the development of an organisation-wide information security strategy. These information security requirements stem from three main sources, being:

- Firstly, by assessing the risk to the information assets of an organisation;
- Secondly, the legal, statutory, regulatory and contractual requirements to be fulfilled by the organisation, its contractors, trading partners and service providers and;
- Thirdly, the set of principles, objectives and requirements for information handling, processing, storing, communicating and archiving that an organisation has developed to support its operations (ISO/IEC27002, 2013, p v; Gerber & Solms, 2001).

The information security requirements of an organisation are established by conducting an information security requirements analysis, as reported in ISO/IEC27003 (2010). However, Van Niekerk and Labuschagne (2006), report that most well-known information security best practices and standards, such as the ISO/IEC27000 family, are too complex and resource intensive for SMMEs to implement.

Therefore, this research study was conducted to develop a simpler method for SA SMMEs to establish their unique information security requirements. The researcher therefore set out to discover four factors that could influence the design and development of this simpler method. Firstly, to understand the perspective of various literature on the use of information security requirements and what they are (*perspective*). Secondly, the definition of information security requirements, from information security best practices and standards (*criteria*). Thirdly, the core elements of an artefact developed for SMMEs (*core elements*). Fourth and finally, the researcher established what the outcomes of effective information security governance are (*outcomes*), to ensure that the developed method will contribute to effective information security governance.

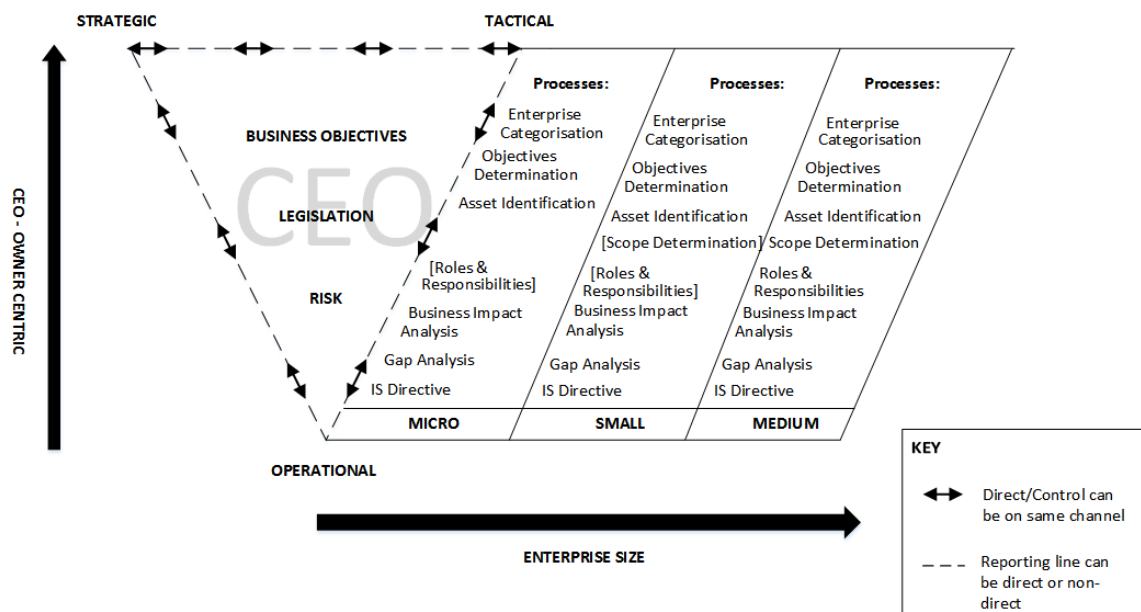
Upon discovering the perspective, criteria, core elements and outcomes, a survey was conducted. The purpose of the survey was to confirm the existence of the phenomena discovered through the literature survey, in an SA SMME context. Through the few responses received from the survey, the phenomena appeared to exist in the SA SMME context too. Therefore, the perspective, criteria, core elements and outcomes were used to derive seven draft principles. These draft principles are required by the research design that was used to conduct the research study, namely design-based research (Herrington, McKenney, Reeves, & Oliver, 2007).

The seven draft principles, as seen below, guided the design and development of the model, which forms the contribution (output) of this research study:

1. **Strategic alignment**- to ensure that the information security efforts of the organisation are aligned with the business strategy, principles and objectives for information security governance.
2. **Risk control**- clearly showing how information security risk management decisions are made within the organisation, giving executive level management an insight on these decisions.
3. **Feasibility**- making the model implementable even under the limited financial resources, human resources and expertise of SMMEs.
4. **Performance measurement**- using information security requirements as a metric to measure the effectiveness of the implemented information security controls of an organisation.
5. **Utility**- in preventing the over-management of information security risks, the model should allow for the optimisation of information security investment according to the size and level of maturity of the organisation.
6. **Simplicity**- the processes of the model to determine information security requirements, should be easily integrated with the business processes of the organisation rather than using information security best practices and standards.
7. **Due diligence**- the model should depict how an organisation took reasonable steps to establish and understand its information security requirements and what decisions were taken regarding its established information security requirements.

## The Model

As discussed above, these draft principles were used to guide the design and development of a model known as the Model for the Alignment of Information Security Requirements within SA SMMEs (MAISRSS). The MAISRSS, is proposed as a simpler method for SA SMMEs to establish the unique information security requirements of the organisation that are aligned with the business strategy, principles, objectives and business requirements for information processing. Seen in Figure 1, below, is the MAISRSS.



**Figure 1: The Model for the Alignment of Information Security Requirements within SA SMMEs (MAISRSS)**

As seen in Figure 1, above, the MAISRSS is structured in such a manner that it is representative of both the flexible and informal, CEO-owner centric corporate governance management structure reported by Hankinson, Bartlett and Ducheneaut (1997); and the SMME organisational structure described by Beaver and Prince (2004). Thus, the MAISRSS provides utility for the organisation even as it grows in size and matures in its business processes.

The processes of the MAISRSS, are based on guidance for the development of an ISMS as seen in ISO/IEC27001 (2013) and ISO/IEC27003 (2010) and the information security risk management standard (ISO/IEC27005, 2011). A few of the processes are optional for some categories of SMMEs, while mandatory for others. The optional processes are indicated by means of square braces [ ]. All eight of the processes are influenced by the draft principles. The eight processes are as discussed below:

1. **Enterprise categorisation-** Calder (2009, p 36), claims that the scope of an ISMS depends on the size of the organisation, with smaller organisations including everything in the scope of the ISMS. Likewise, the information security requirements will be determined for the information assets within the scope of the ISMS. Additionally, to provide utility it is necessary to support the scalability of the rapidly evolving SMMEs. For this reason, the category of SMME is established according to criteria, as specified in the National Small Business Act of 1996, in order to categorise an organisation as micro, small or medium.
2. **Objectives determination-** compulsory to all categories of SMMEs, supports the draft principle of strategic alignment by assisting organisations to determine their information security objectives and principles.
3. **Asset identification-** is a process with the objective of identifying information assets within the scope of the ISMS, which an organisation must protect. Thereby addressing the risk control, due diligence and simplicity draft principles.
4. **Scope determination-** addresses the draft principles of utility, feasibility and simplicity by ensuring that the scope of the ISMS includes only what is necessary to meet its information security objectives and principles.

5. **Roles and responsibilities-** concerning the protection of information assets are assigned to individuals or departments with the organisation. Thus, this process addresses the feasibility, risk control and utility draft principles.
6. **Business impact analysis-** is a process to measure the potential impact that a successful information security threat could have on the organisation and its operations. This process is related to the draft principles risk control, due diligence and utility.
7. **Gap analysis-** is a process performed to determine whether or not the organisation has met its information security objectives and principles. This process also determines whether current information security efforts are effective in protecting the information assets of the organisation. Therefore, this process relates to risk control, performance measurement, due diligence, utility and strategic alignment.
8. **IS directive** – is the final process and the one in which the information security requirements and the intent to fulfil these information security requirements is communicated by the executive management of the organisation. This process addresses all of the draft principles, as a high level information security policy is generated and details the outcomes of the previous processes, which addressed the draft principles as discussed above. The output of this process is a policy document with the level of information security required for the identified information assets of the organisation and how these information security requirements will be met.

### **The Automated Tool**

The processes of the MAISRSS were incorporated into an automated tool, which was developed based on the MAISRSS. Microsoft Excel was used to develop a prototype of an automated tool that can be developed based on the MAISRSS. A prototype is defined as a simple example of a system, which showcases the practicality and feasibility of the model or framework on which the prototype is based (Olivier, 2009, p. 51). Refer to the video accompanying this document, for a demonstration of the automated tool.

### **References**

- Beaver, G., & Prince, C. (2004). Management, strategy and policy in the UK small business sector: a critical review. *Journal of Small Business and Enterprise Development*, 11(1), 34–49.  
<https://doi.org/10.1108/14626000410519083>
- Brotby, K. (2009). *INFORMATION SECURITY GOVERNANCE INFORMATION SECURITY GOVERNANCE A Practical Development and Implementation Approach*. New Jersey: John Wiley & Sons, Inc.  
 Retrieved from <http://www.wiley.com/go/permission>.
- DTI. (2006). *Information security : Protecting Your Business Assets*. London. Retrieved from <http://webarchive.nationalarchives.gov.uk/20060213212102/dti.gov.uk/bestpractice/assets/security/ispyba.pdf>
- Gerber, M., & Solms, R. Von. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, 20, 577–584.
- Hankinson, A., Bartlett, D., & Ducheneaut, B. (1997). The key factors in the small profiles of small-medium enterprise owner-managers that influence business performance: The UK (Rennes)

SME survey 1995-1997 An international research project UK survey. *International Journal of Entrepreneurial Behavior & Research*, 3(3), 168–175.

Herrington, J., McKenney, S., Reeves, T. C., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal. In *World Conference on Educational Multimedia, Hypermedia and Telecommunications* (pp. 4089–4097). Chesapeake, VA. Retrieved from <http://ro.ecu.edu.au/ecuworks/1612>

ISO/IEC. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

Iso/iec27002. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

ISO/IEC27003. (2010). *Information technology — Security techniques — Information security management system implementation guidance*. Geneva.

ISO/IEC27005. (2011). *Information technology — Security techniques — Information security risk management*. Geneva.

Olivier, M. S. (2009). *Information Technology Research 3*. (M. Marchand, Ed.) (3rd ed.). Pretoria: van Schaik.

Peltier, T. R. (2004). Information security policies and procedures, (June), 412. Retrieved from <http://books.google.co.nz/books?id=TDg2tHV6BNMC>

Posthumus, S., von Solms, R., & King, M. (2010). The board and IT governance : The what , who and how. *Framework*, 41(3), 23–33. Retrieved from [http://www.sabinet.co.za/abstracts/busman/busman\\_v41\\_n3\\_a4.html](http://www.sabinet.co.za/abstracts/busman/busman_v41_n3_a4.html)

Van Niekerk, L., & Labuschagne, L. (2006). The PECULIUM model: information security risk management for the south african SMME.

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

Yolande Smit. (2012). A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African Journal of Business Management*, 6(21), 8233. <https://doi.org/10.5897/AJBM11.2709>



### **D.3 SMME Expert Interview: Questionnaire**

Similar to the information security expert's suite of information, the SMME expert was also given a questionnaire as a guide to conduct the evaluation. The questionnaire given to the SMME expert varied slightly from the one given to the information security expert. Variations include that the SMME expert interview questionnaire asked specifically about the automated processes; while the information security expert interview questionnaire asked about the usual (not automated) processes.

# An Automated Tool for the Alignment of Information Security Requirements within SA SMMEs

Evaluation Survey Questionnaire

September 2018

## Background Information

*This section of the questionnaire pertains to information relating to the qualifications and experience of the SMME representative evaluating the attached automated tool. In addition, questions 3 to 6 seek to categorise the enterprise according to criteria from the National Small Business Act of 1996.*

1. Please provide your name, surname and title (e.g. Mr, Miss, Mrs, Dr, Prof., etc.) [optional].

Name	Surname	Title

2. What is your current occupation and job title/description within the enterprise?

Occupation	Job Title/Description

3. Is your enterprise or the head office of your enterprise situated in South Africa?
- Yes
  - No
4. Is your enterprise part of a franchise or chain store organisation?
- Yes
  - No
5. How many full-time, paid employees does your enterprise currently employ?
- 0-5
  - 6-10
  - 11-20
  - 21-30
  - 31-50
  - 51-200
  - 200 or more
6. What is the average annual turnover of your enterprise?
- 0-150k
  - 151k-400k
  - 401k-1m
  - 1.1m-2m
  - 2.1m-3m
  - 3.1m-5m
  - 5m-10m
  - 10.1m-15m
  - 15.1m-50m

- j. 51m or above
7. What is the average value of total gross assets owned by your enterprise?
- a. 0-150k
  - b. 151k-400k
  - c. 401k-1m
  - d. 1.1m-2m
  - e. 2.1m-3m
  - f. 3.1m-5m
  - g. 5m-10m
  - h. 10.1m-15m
  - i. 15.1m-50m
  - j. 51m or above

Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box. Indicate your selection by ticking, highlighting or underlining your selection.

8. Please rate the extent to which the highest academic qualification that you possess, relates to information security or information security governance.

Strongly related	Related	I am not sure	Somewhat related	Completely unrelated
------------------	---------	---------------	------------------	----------------------

9. How many years of experience do you have, working in the SMME sector?

years.

10. Based on your experience and knowledge, to what extent would you agree that you are confident in answering questions related to information security and/or information security governance in your enterprise?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

11. Please indicate the extent to which you are confident in your knowledge and ability to answer questions related to SMMEs.

Very confident	Confident	Neutral	Not so confident	Not confident at all
----------------	-----------	---------	------------------	----------------------

## General Principles

Refer to Appendix A: Background information, to answer questions 7 to 13. The General Principles section attempts to establish the understanding and opinion of the SMME representative, evaluating the automated tool, pertaining to the research problem to be solved by this research study.

Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box. Indicate your selection by ticking, highlighting or underlining your selection.

12. Please indicate the extent to which you agree that an enterprise should exhibit transparency on how directives from executive management link to implemented information security controls.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

13. Please indicate the extent to which you agree that it is necessary for the executive management of an enterprise, to clearly define how decisions on information security risks are made within the enterprise.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

14. Please indicate the extent to which you agree that most information security best practices and standards are not feasible for SMMEs to use, due to resource constraints.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

15. Please indicate the extent to which you agree that information security requirements should be used as a metric to measure the performance of implemented information security controls.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

16. In your experience, how often is it that a tool needs to be scalable to various sizes and levels of maturity of enterprises, to be useful to most SMMEs?

Very frequently	Frequently	Occasionally	Rarely	Never
-----------------	------------	--------------	--------	-------

17. To what extent do you agree that the characteristics and constraints of SMMEs require that any tool, policies, regulations or standards developed for these enterprises should be simple?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

18. In your opinion, to what extent is it important for an enterprise to prove that due diligence was done pertaining to the control of information security risks, to avoid legal liability?

Very Important	Fairly Important	Important	Slightly Important	Not at all Important
----------------	------------------	-----------	--------------------	----------------------

## Draft Principles

Refer to the Appendix A: Background Information and the attached video file, to answer the questions that follow. This section of the questionnaire attempts to assess the extent to which the SMME representatives, agree that the automated tool adheres to the draft principles which guided the design and development of the model on which the automated tool is based.

Please rate how strongly you agree or disagree with each of the following questions by placing an **X** in the appropriate box. Indicate your selection by ticking, highlighting or underlining your selection.

19. To what extent do you agree that the automated tool demonstrated in the video, provides a method simple enough to determine the information security requirements of your enterprise with ease?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

20. Please indicate the extent to which you agree that the automated tool is useful to your enterprise currently and will remain so, as the enterprise grows and matures.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

21. Please indicate how confident you are that the information security requirements generated by the automated tool can provide accurate metrics to evaluate the performance of the information security controls implemented by the enterprise.

Very confident	Confident	Neutral	Not so confident	Not confident at all
----------------	-----------	---------	------------------	----------------------

22. In your opinion, to what extent do you agree that the processes of the automated tool can be performed even in enterprises with minimal resources such as SMMEs?

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

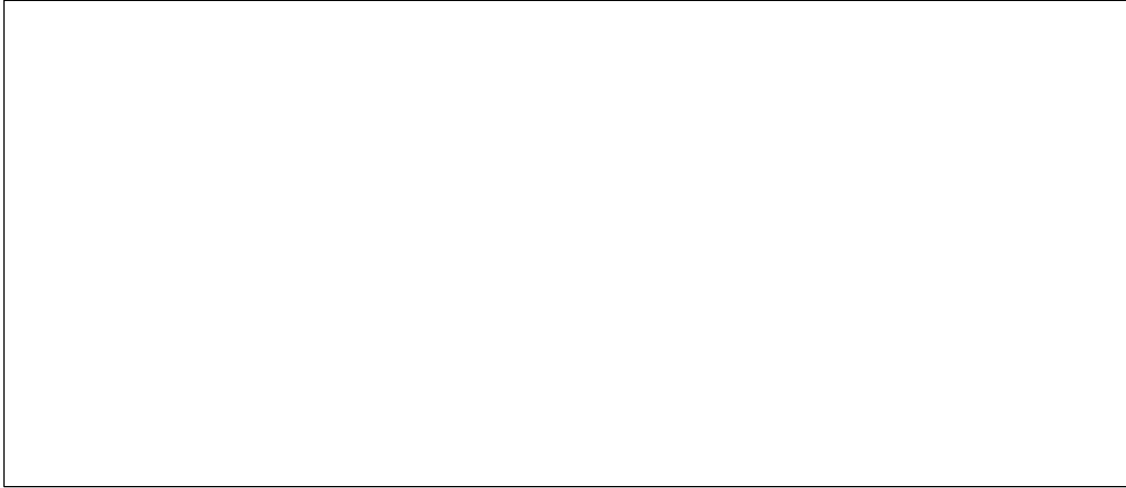
23. Please indicate the extent to which you agree that the information security requirements established through the automated tool will clearly link the need of the enterprise to the implemented information security controls.

Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree
----------------	-------	---------------------------	----------	-------------------

24. In your opinion, to what extent do the processes of the automated tool ensure that the information security requirements generated, reflect the vision for the enterprise as set out by the executive management of the enterprise?

Excellently	Good	Adequate	Fair	Poor
-------------	------	----------	------	------

25. Please provide any suggestions, recommendations or opinions that could assist the researcher in improving the automated tool and its suitability to SA SMMEs.

A large, empty rectangular box with a thin black border, intended for the respondent to provide their suggestions, recommendations, or opinions. The box is currently blank.

**Thank you for your time and invaluable participation.**

# Appendix E

## Academic Publications

During the research conducted towards this dissertation, a peer-reviewed paper was written and submitted for presentation at a national conference (the paper was not successful in being selected for presentation due to information security requirements being misunderstood by one of the reviewers as the requirements of a software application or requirements engineering, which caused the paper to be rejected. This paper will be reworked to state the information security focus more explicitly, as to avoid any potential misunderstanding of it as requirements of a software application or requirements engineering and will be submitted to another forum for review). The paper is as seen below:

# Towards a model for the alignment of information security requirements in South African SMMEs

**Abstract**—Small, Micro and Medium Enterprises are dynamic, with the possibility of fast growth or failure. These enterprises face a number of challenges to their existence, such as a lack of resources, a lack of governance skills and many others. Thus making it hard for them to properly implement information security and understand their information security requirements. This research paper presents a model designed to assist South African Small, Micro and Medium Enterprises to align their information security requirements with the business objectives of the enterprise and with the higher management levels. The Design-oriented Information Systems research methodology was used for this research project.

**Keywords:** SMME, information security, information security requirements, information security governance

## I. INTRODUCTION

Enterprises, implement information security in an attempt to make their information secure against malicious attacks [1]. However information security solutions implemented by enterprises are often designed, acquired and implemented on a tactical basis, to meet a specific situation. This often results in a multitude of technical solutions, each independently designed, with no consideration of the strategic dimension or the goals of the business [2]. Although information security management standards such as ISO 27002 exists to assist enterprises in developing and implementing information security, the adoption of these standards is not a straight forward process for any enterprise, let alone an SMME [3]. Tailoring information security best practices and standards to the information security requirements of an enterprise could result in a business-driven information security architecture, which describes a structured inter-relationship between the technical and procedural solutions to support the long-term business needs of the enterprise [4].

This paper describes a model developed to assist South African (SA) small, micro and medium enterprises (SMMEs) in tailoring information security best practices and standards to their information security requirements. The model was developed with the varying management structures of SMMEs in mind and the low resources found in these enterprises. In presenting the need for the model, this paper begins with a discussion of information, corporate governance, the corporate governance of information and communication technology and information security governance, This paper further goes on, to discuss what information security requirements are, what SMMEs are, particularly in an SA context, as well as their management structures. The research methodology used

for this study will also be mentioned, before the proposed model is introduced.

## II. INFORMATION SECURITY GOVERNANCE

Before defining and discussing information security governance, it is necessary to understand what information, corporate governance and the corporate governance of information and communication technology are. Therefore this section discusses these concepts in that order.

### A. Information

Computers and the use thereof have evolved rapidly over time. More importantly their role and use in enterprises has also evolved greatly, due to benefits provided by information and communication technology (ICT) such as competitive advantage and timely access to information among others. This evolution has brought about great change, with a shift from the computer-centric era where the physical protection of the ICT infrastructure was the main concern, to an information-centric era, where information is reported to be the life-blood of an enterprise [5; 6]. In this information-centric era, useful data, known as information is reported to be one of the most critical strategic assets of an enterprise. Failure to adequately protect the information assets of an enterprise could result in calamitous risks, even including the demise of an enterprise. Therefore, the protection of this information and its related technology is reported to form part of the corporate governance responsibility of an enterprise [7; 8; 9].

### B. Corporate Governance

Corporate governance is the relationship between the various participants involved in determining the direction and ensuring the performance and well-being of an enterprise, also referred to as the system by which the enterprise is directed and controlled [10; 11; 12; 9; 13]. The participants of corporate governance can be grouped into three main levels of management, namely: strategic-level management (board of directors and executive management, who provide the enterprise with direction in the form of directives); tactical-level management (middle-level management, who translate the directives received from strategic management and implement them as policies, procedures and company standards); and operational-level management (lower-level management, responsible for ensuring the implementation of the policies, procedures and company standards in the day to day operations of an enterprise) [9]. Corporate governance is



concerned with the performance and well-being of an enterprise; thus it is imperative that the well-being of assets which are critical to the survival of the enterprise and related technology (ICT) form part of the corporate governance structure.

#### *C. Information and Communication Technology Governance*

ICT governance is a component of corporate governance and is the structure through which management of an enterprise attempts to ensure that the enterprise's ICT investment is strategically aligned with the objectives of the enterprise and is used in a manner that mitigates the associated risks [13; 9; 14; 15].

However the security achieved purely through technical means and by only addressing risks to the ICT is limited, as it often only addresses the security needs of the hardware and infrastructure and not those of the information. Business or personal information needs to be protected wherever it resides [16; 17].

#### *D. Information Security*

Therefore it is necessary to protect the information from inadvertent or malicious changes, deletions or unauthorised disclosure. This is known as information security and in full is defined as "all the aspects related to achieving and maintaining confidentiality, integrity, availability, accountability, authenticity and reliability" [17].

Information security is such an important aspect of an enterprise that it should be addressed at an executive management level [18].

#### *E. Information Security Governance*

The process of governing information security at an executive level is known as information security governance [18].

However it has been reported that many enterprises design and install information security solutions on a tactical basis. This results in a build-up of a mixture of technical solutions on an ad-hoc basis. These independently developed solutions have no guarantee that they will be compatible and interoperable or even worse that they can support the goals of the business [2]. "The solution would be the development of an enterprise security architecture, which is business driven and describes a structured inter-relationship between the technical and procedural solutions, to support the long-term business needs of the enterprise. This requires a thorough understanding of the information security requirements of the enterprise" [2].

### III. INFORMATION SECURITY REQUIREMENTS

Information security requirements can be defined as "the amount of security needed to provide the required level of information security." This can be interpreted as the security concerns of the enterprise, combined with the level of security required for each concern, resulting in the information security requirements [5].

Information security requirements provide management with a starting point in the development of an enterprise-wide information security strategy. These information security requirements stem from three main sources, being: Firstly,

assessing the risk to the enterprise; Secondly, the legal, statutory, regulatory and contractual requirements to be fulfilled by the enterprise, its contractors, trading partners and service providers and; Thirdly, the set of principles, objectives and requirements for information handling, processing, storing, communicating and archiving that an enterprise has developed to support its operations [16; 5].

Information security requirements feature at different levels of management within an enterprise. The detail of the information security requirements varies according to the level of management. The information security requirements are communicated via the inter-tier and intra-tier communications, in the same way that business directives are communicated through the enterprise management structure [19].

With reports of information security solutions being designed, acquired and implemented on an ad-hoc basis, there is an indication of misalignment or lack of communication of the strategic directives and the rest of the enterprise [2; 20].

Unclear information security requirements can often lead to coping methods such as non-compliance. This non-compliance can be implementation of technology and solutions on an ad-hoc basis, just to get the job done or a complete disregard of tasks set out to fulfill the information security requirements [20].

Although information security best practices and standards exist to assist enterprises in the development of an enterprise information security architecture they are reported to be resource intensive and complex to implement if treated purely as technical guidance. Therefore management and staff must understand what to do, how to do it and why it is important. This task is often daunting for enterprises without the proper know-how or expertise to understand and implement these best practices and standards [4].

### IV. SMALL MICRO AND MEDIUM ENTERPRISES

Small Micro and Medium Enterprises (SMMEs) often face a number of challenges including a lack of financial resources and extended human resource, among many others. The adoption of information security best practices and standards is not a straightforward process for a company, least so far for an SMME [21; 3]. Devos, van Landeghem and Deschoolmeester [15], claim that "the concept of IT governance originates from the discussion of strategic ICT planning and ICT management, but its link to corporate governance is often a "bridge too far" for most SMMEs".

Information security governance is a subset of ICT governance [18]. Therefore it can be assumed that it is equally challenging for SMMEs to bridge the gap between corporate governance and information security governance.

Many authors state that the definition of SMMEs varies widely according to a number of factors. A few factors which have been used to classify an enterprise as an SMME are size (number of employees), annual turnover and the type of ownership of the enterprise [22].

A common theme in SMME literature is that these enterprises are reported to have a lack of resources, which makes them unable to afford the expertise required to implement

information security [21; 23]. The National Small Business Act of South Africa [24], defines an SMME as “a separate and distinct business entity, including cooperative enterprises and non-governmental enterprises, managed by one owner or more which, including its branches or subsidiaries, if any, is predominantly carried on in any sector or subsector of the economy mentioned in column I of the Schedule and which can be classified as a micro-, a very small, a small or a medium enterprise”. This research paper focuses on the micro, small and medium categories of enterprises.

Table 1. Summary of NSBA Schedule (NSBA, 1996)

Size or class (Categories)	Total full-time equivalent of paid employees	Total annual turnover/Revenue In R (million)	Total gross asset value (fixed property excluded) In R (million)
Micro	5	0.15	0.1
Very small	20	5	1.8
Small	50	25	4.5
Medium	200	50	18

Therefore, the authors of this paper propose a model to assist South African SMMEs in bridging the gap between corporate governance and information security governance, by providing guidance on aligning information security requirements at the various enterprise management levels.

## V. RESEARCH METHODOLOGY

Similar to most studies in the information security field, this study adopts the qualitative rather quantitative research approach. This research paper forms part of a larger research project which follows the design-oriented information systems (IS) research methodology, as defined by Österle, et al., [25].

Design-oriented IS research methodology is non-prescriptive of specific research methods to be followed and aims at the development of artifacts, such as constructs, models and instantiations, while ensuring scientific rigor and practical relevance [25; 26].

Therefore, design-oriented IS research projects must comply with four basic principles [25]:

*a) Abstraction:* Each abstract must be applicable to a class of problems. The model designed by this research project particularly addresses the problem of information security requirements alignment in South African SMMEs.

*b) Originality:* Each artifact must substantially contribute to the advancement of the body of knowledge. Although other such works may exist, few attempt to understand the needs of the different categories of SMMEs,

considering the three sources of information security requirements.

*c) Justification:* Each artifact must be justified in a comprehensible manner and must allow for its validation. The model is based on the corporate governance model, while incorporating three of the four categories of SMMEs, as stated in the National Small Business Act [24] and the three sources of information security requirements as set out in various literature and information security best practices and standards. As part of the larger project this model will be evaluated by means of an expert review.

*d) Benefit:* Each artifact must yield benefit, either immediately or in the future, for the respective stakeholder groups. The benefit of this model can be seen both immediately and in the future based on proper implementation and understanding of the model.

The design-oriented research methodology consists of four phases for a research project [25]:

*a) Analysis:* business problem identified and described, research objectives, questions, and gaps are specified. The research plan is put forward for the development and improvement of the required artifacts. For this a literature review was conducted. Literature included published works on the implementation of information security in SMMEs, challenges faced by South African SMMEs, the adoption of information security best practices and standards in SMMEs, the management structure of SMMEs and some other literature.

*b) Design:* the artifacts are created through generally accepted methods. The developed artifacts must be justified and contrasted with known solutions, which already exist. Few known models and frameworks of this kind exist. Thus this phase of the research project relied on the identification and abstraction of ideas from similar projects of relevance. These ideas were then evaluated based on the sources for information security requirements, the challenges facing SMMEs and other constraints established through literature. A combination of these results and the characteristics of SMMEs taken from literature, resulted in the proposed model.

*c) Evaluation:* the scientific rigor of the artifact is validated against the objectives specified, applying the methods stated in the research plan. As previously stated, this paper forms part of a larger research project. In the larger research project, methods such as a semi-structured interview and an elite interview will be conducted in two different rounds, to ensure the usefulness and rigor of the model.

*d) Diffusion:* the phase in which the findings from the research are produced/published. Design-oriented IS research mainly uses the following methods of diffusion: conference papers, technical books, dissertation thesis, among a few

others. The findings from the research project will be published in conference proceedings such as this one, by means of journal publications and through the writing of a dissertation.

## VI. MODEL FOR THE ALIGNMENT OF INFORMATION SECURITY REQUIREMENTS

Fig. 1 is the model proposed by the authors of this paper, to assist SMMEs in the alignment of their information security requirements at the three management levels.

The model is based on the corporate governance model, while incorporating three of the four categories of SMMEs with small and very small being combined as one.

This section will discuss the components of the model.

a) *Guidelines/Checklist:* a set of guiding statements will be provided for the user of the model to understand what the typical outcome would be at their level. These guidelines will be devised using information security best practices and standards, as well as literature sources. The checklist will consist of tasks which can be checked off to measure progress and ensure that the correct procedure is followed by the user. The guidelines and checklist will ensure that only the legal, risk and objectives applicable to that category of SMME with a specific management structure are selected.

b) *Categories of SMMEs:* SMMEs exist in various sizes but are categorised according to the four categories as mentioned earlier in this paper. It is therefore understood that although one startup SMME might only have a single employee who is also the owner and manager, another startup SMME might have far more employees occupying these roles. It is thus understood that a single and simple management structure for all SMMEs would not be accurate. Although only three of the four SMME categories are presented, this model is therefore dynamic in that it allows the user to use only the applicable aspects according to the management structure of their SMME, without any additional know-how and expertise being required.

c) *Source of information security requirements:* the three sources from which information security requirements stem are the same for all sizes of enterprise. What varies is the level of detail and applicability according to the specific industry and the size of the enterprise. The three sources also do not become different at each of the management levels, but their detail and target audience becomes different. Therefore it is necessary that the information security requirements are appropriately interpreted to be appropriately understood by the correct audience / management level. Thus combined with the checklists and guidelines, users of this model will be able to determine what level of detail they should go into when establishing a specific information security requirement and what to include when preparing to have the information security requirements translated to a lower management level.

d) *Enterprise management levels:* SMMEs are dynamic in nature and vary in their structure. Therefore this model must provide for scalability and the dynamic nature of SMMEs. Specific clauses of best practices and standards are applicable to the various industries at each of the three management levels. From governance, to management each varies according to the information security requirements, industry and level of management. Questions asked at each of these management levels, provide answers which should form part of the overall vision and business objectives of the enterprise.

- *Why?* This question is asked by the strategic level management in determining the reason for investment. This question should be aligned with the vision and mission of the business, as set out by strategic level management. This will provide guidance to the entire enterprise and motivate them to comply with the efforts of the enterprise.
- *What?* The tactical level management is responsible for interpreting directives and strategic management statements into policy, procedures and company standards. At this level of management the question asked is, what do we need to implement to achieve the vision of strategic management? Here information security best practices and standards which are applicable to the enterprise are selected. These will vary according to the industry and business objectives of the enterprise, therefore tactical level management must understand what the intention of strategic level management is for the enterprise and for information security.
- *How?* Although it is a question answered by tactical level management in drawing up the procedures to be implemented at the operational level, operational level managers ask themselves on a daily business how they can keep the enterprise moving forward. The answer to this question often comes in the form of information security controls which should be implemented and maintained.

Each of these components of the model play a vital role in ensuring that SMMEs of all sizes are able to determine their information security requirements even with limited knowledge about information security, limited access to financial resources and not many employees. A combination of questions, statements and other guidance from literature, information security best practices and standards will be used to provide the correct mapping of SMME to the tasks that should be completed to obtain the information security requirements at an adequate level.

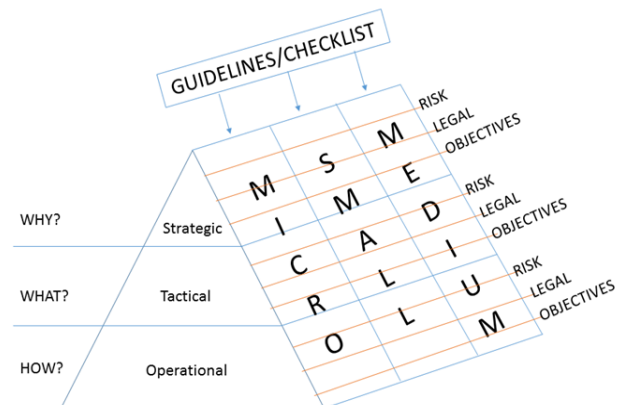


Figure 1. SMME information security requirements alignment model

## VII. CONCLUSION

The need for information security has grown as information has become a critically important strategic asset in most enterprises. A breach in the security of information is reported to be of detriment to an enterprise, even leading to the demise of an enterprise. Furthermore information security should be implemented by means of an enterprise-wide architecture, which is business driven. Therefore the information security solutions of the enterprise must be aligned with the business objectives of the enterprise.

Information security best practices and standards attempt to assist enterprises in the development of such enterprise information security architecture. However it is reported that these best practices and standards can be complex and resource intensive for SMMEs to implement. Therefore a model was proposed to assist SMMEs in ensuring the alignment of information security requirements at the various enterprise management levels, thereby simplifying the implementation of information security best practices and standards. The model is based on the corporate governance model and incorporates the different categories of SMMEs. SMME owners can use the guidelines or checklists to verify the information security requirements at each management level of the enterprise. Future research could see this model transformed into a framework with guidance on determining the information security requirements.

## VIII. REFERENCES

- [1] Calder, Alan. Implementing Information Security based on ISO 27001/ISO 27002 A Management Guide. [ed.] Jan van Bon and Selma Polter. s.l. : Van Haren Publishing, 2009.
- [2] SALSA: A Method for Developing the Enterprise Security Architecture and Strategy. Sherwood, John. 15, Sussex : Elsevier Science, 1996, Computers & Security , pp. 501-506.
- [3] IT Governance Institute, Office of Government Commerce. Aligning CobiT 4.1, ITIL v3 and ISO/IEC 27002 for business benefit. United States of America : Crown Copyright, 2008.
- [4] ISO/IEC38500. Corporate Governance of Information Technology. s.l. : ISO, 2008.
- [5] International Organization for Standardization, International Electrotechnical Commission. Corporate Governance of Information Technology. ISO/IEC 38500. s.l. : ISO/IEC, 2008.
- [6] ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls. ISO/IEC 27002. Switzerland : International Organization for Standardization, 2013.
- [7] Institute of Directors Southern Africa. King Code of Governance for South Africa 2009. s.l. : Institute of Directors Southern Africa, 2009.
- [8] National Small Business Act . NO. 102 OF 1996: NATIONAL SMALL BUSINESS ACT, 1996. National Small Business Act . s.l. : Parliament of South Africa, 1996.
- [9] Organization for Economic Cooperation and Development. OECD Corporate Governance Principles. s.l. : OECD, 2015.
- [10] National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 4. Gaithersburg : National Institute of Standards and Technology, 2013.
- [11] Corporate governance and the small and medium enterprises sector: theory and implications. Abor , Joshua and Adjasi, Charles K D. 2, s.l. : Emerald Insight, 2007, Corporate governance: The international journal of business in society , Vol. 7, pp. 111-122.
- [12] Issues in Implementing IT Governance in Small and Medium Enterprises . Ayat, Masarat, et al. s.l. : IEEE, 2011.
- [13] Exploring the suitability of IS security management standards for SMEs. Barlette , Yves and Fomin, Vladislav V. Hawaii : IEEE, 2008. pp. 3-10.
- [14] Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. D'Arcy, John, Herath, Tejaswini and Shoss, Mindy K. 2014, Journal of Management Information Systems, pp. 285-318.
- [15] Rethinking IT governance for SMEs. Devos, Jan, van Landeghem, Hendrik and Deschoolmeester , Dirk. 2, s.l. : Emerald Insight, 2012, Industrial Management & Data Systems, Vol. 112.
- [16] From Risk Analysis to Security Requirements. Gerber , Mariana and von Solms , Rossouw. Port Elizabeth : Elsevier Science, 2001, Computers & Security, Vol. 20, pp. 577-584.
- [17] Formalizing information security requirements. Gerber , Mariana , von Solms, Rossouw and Overbeek, Paul. 1, s.l. : Emerald Insight, 2001, Information Management and Computer Security , Vol. 9, pp. 32-37.
- [18] Monks, R A and Minow, N. Corporate Governance Blackwell. Cambridge : s.n., 1995.
- [19] A method for researcher-practitioner collaboration in design-oriented IS research. Osterle , Hubert and Otto, Boris. 2010.
- [20] [20].Memorandum on design-oriented information systems research. Osterle , Hubert , et al. 2010, European Journal of Information Systems, pp. 1-4.
- [21] A framework for the governance of information security. Posthumus, Shaun and von Solms , Rossouw. s.l. : Elsevier Ltd, 2004, Computers & Security , Vol. 23, pp. 638-646.
- [22] SMME Development in Johannesburg's Southern Metropolitan Local Council: An Assessment. Rwigema, H and Karungu, P. 1999, Development South Africa, pp. 107-127.
- [23] A literature review of small and medium enterprises (SMEs) risk management practices in South Africa. Smit, Yolande and Watkins, J A. 2012, African Journal of Business Management, pp. 6324-6330.
- [24] The information security management toolbox- taking the pain out of security management. Vermeulen, Clive and von Solms , Rossouw. 3, s.l. : Emerald Insight, 2002, Information & Computer Security , Vol. 10, pp. 119-125.
- [25] von Solms, S H and von Solms, R. Information Security Governance. New York : Springer Science, 2009. ISBN: 978-0-387-79983-4.
- [26] Whitman, Michael E and Mattord, Herbert J. Principles of Information Security. 4th. Boston : Cengage Learning, 2012. p. pg10.

# Appendix F

## Language Quality Assurance Certificate

**Language Quality Assurance Practitioner  
(Professional language editor)**

Dr PJS Goldstone  
22 Invicta Ave.  
Berea,  
Durban.  
  
South Africa

Cell: 073-196-0087

pat@pemail.co.za

30<sup>th</sup> November 2018

**TO WHOM IT MAY CONCERN**

We hereby certify that we have language-edited the dissertation of Timothy Harambee Speckman titled: A MODEL FOR THE ALIGNMENT OF INFORMATION-SECURITY REQUIREMENTS WITHIN SOUTH AFRICAN SMALL, MEDIUM AND MICRO-ENTERPRISES..

We are satisfied that, provided the changes we have made are effected to the text, the language is of an acceptable standard, and is fit for publication.



**Kate Goldstone**

BA (Rhodes)

SATI No: 1000168

UPE Language Practitioner (1975-2004)

NMMU Language Practitioner (2005)



**Dr Patrick Goldstone**

BSc (Stell.)

DEd (UPE)