

**A FRAMEWORK FOR CYBER SECURITY  
AWARENESS IN SMALL, MEDIUM AND  
MICRO ENTERPRISES (SMMES) IN SOUTH  
AFRICA**

by

**Tebogo Lejaka**

for the degree of

**MASTER OF SCIENCE**

in

**COMPUTING**

at the

**University of South Africa**

Supervisor: Prof Adéle da Veiga

Co-Supervisor: Prof Marianne Look

Date: October 2021

## ABSTRACT

In South Africa, there is a rapid increase of cyber attacks intended for organisations regardless of size and industry. Cyber attacks are directed at businesses of all sizes; however, small, medium and micro enterprises (SMMEs) are impacted most because of limited information technology (IT) skills and financial support to prevent cyber threats. There is a significant increase in SMMEs in South Africa which are important because of their contribution to the country's economy. Organisations, including SMMEs, are converted gradually to depend on IT to sustain their competitive advantage and boost services. In South Africa, many organisations, including SMMEs, are still not effectively prepared to prevent cybercrimes. Therefore, there is a need to create cyber security awareness for SMMEs because they have a direct impact on the cyber security infrastructure of the country. Based on systematic literature review findings, a research gap has been identified whereby a cyber security awareness study has not been conducted for South African SMMEs where a suitable model and framework for raising cyber security awareness for SMMEs in South Africa have been developed. The main aim of the research study is to develop a framework for cyber security awareness for South African SMMEs (Csa4Smmes {RSA} framework). This research study follows the design science research methodology (DSRM) approach. This approach is most suitable and carefully selected to address the purpose of the study. Models and frameworks have been evaluated to develop components of the conceptual Csa4Smmes {RSA} framework which are used as building blocks to develop the intermediate Csa4Smmes {RSA} framework. Semi-structured interviews with experts in cyber security, science and technology awareness as well as SMMEs management and operation were conducted to demonstrate and evaluate the intermediate Csa4Smmes {RSA} framework. Consequently, this framework was produced as an artefact to enhance cyber security awareness levels within SMMEs in South Africa. Cyber security awareness has been demonstrated to be an effective approach to enhance cyber security awareness level. Therefore, the Csa4Smmes {RSA} framework can assist government in reducing cyber attacks associated with internet users.

## KEYWORDS

Cyber security awareness, SMMEs, SMEs, small businesses, design science research methodology, systematic literature review, Csa4Smms {RSA} framework

## ACKNOWLEDGEMENTS

Firstly, I would like to praise and give thanks to the almighty God for countless blessings, opportunities, and enabling me to carry out this study.

I would like to thank my supervisors, Professors Adéle da Veiga and Marianne Loock, who provided me with guidance and support towards the process of conducting this research. I would also like to thank Professor Marlien Herselman for sharing knowledge and experience regarding design science research.

I would like to give thanks to the Department of Science and Innovation (DSI), the Council for Scientific and Industrial Research (CSIR) and Armscor for financial support towards my studies.

I would also like to thank the CSIR (Cyber security) and the South African Agency for Science and Technology Advancement (SAASTA – Science and Technology Awareness) for allowing their employees to contribute knowledge towards my study. In addition, I appreciate the contributions made by all expert reviewers (including SMME owners) who assisted with demonstrating and evaluating the conceptual framework for cyber security awareness in SMMEs.

I would love to thank my family (Mma, Papa, Itu, and Kedi) and close friends for their exceptional support and constant encouragement. I appreciate and value those (Matsobane, Nthaby and Pontsho) who continuously helped with proofreading my work. Mmaletsema, Tumi and family thanks for your prayers and support. It is much appreciated.

## DECLARATION

I, Tebogo Kesetse Lejaka, hereby declare that this document: [A FRAMEWORK FOR CYBER SECURITY AWARENESS IN SMALL, MEDIUM AND MICRO ENTERPRISES \(SMMEs\)](#), submitted for evaluation towards the requirements of the subject: Cyber security awareness, as part of the Master of Science in Computing qualification at the University of South Africa, is my own original work and has not previously been submitted to any other institution of higher learning or subject for evaluation. All sources used or quoted in this document are indicated and acknowledged by means of a comprehensive list of references.

Surname, Initials: Lejaka TK

Student Number: 46926461

Signature: \_\_\_\_\_

Date: 23/09/2021

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>2</b>
1.1	OVERVIEW OF CHAPTER 1.....	2
1.2	INTRODUCTION.....	2
1.3	BACKGROUND .....	2
1.3.1	What is cyberspace? .....	3
1.3.2	Cyber security, a global concern .....	4
1.3.3	Cyber security in South Africa, a developing country .....	6
1.3.4	Current state of South Africa towards information communication technology 9	
1.3.5	The importance of cyber security awareness .....	11
1.3.6	Audience analysis for cyber security awareness .....	12
1.3.7	Motivation for cyber security awareness.....	12
1.3.8	People are the weakest link.....	12
1.3.9	Challenges faced by SMMEs.....	13
1.4	PROBLEM STATEMENT AND RESEARCH QUESTIONS .....	14
1.4.1	Main research question .....	15
1.4.2	Sub-research questions.....	16
1.4.3	Main research objective.....	16

1.4.4	Sub-objectives .....	16
1.4.5	Importance of the study .....	17
1.5	RESEARCH METHODOLOGY .....	18
1.6	ETHICAL CONSIDERATIONS.....	22
1.7	OVERVIEW OF CHAPTERS .....	23
1.8	SUMMARY.....	24
<b>2</b>	<b>RESEARCH METHODOLOGY.....</b>	<b>26</b>
2.1	INTRODUCTION.....	26
2.2	OVERVIEW OF CHAPTER 2.....	26
2.3	RESEARCH DESIGN PROCESS.....	26
2.3.1	Research philosophy .....	26
2.3.2	Paradigm .....	27
2.3.3	Research approaches.....	29
2.3.4	Research methodology.....	30
2.3.5	Research strategy .....	32
2.3.6	Data collection techniques.....	33
2.3.7	Data analysis .....	36
2.4	DESIGN SCIENCE RESEARCH METHODOLOGY .....	38
2.4.1	Introduction.....	38
2.4.2	Design Science Research Methodology process .....	41

2.4.3	Guidelines for carrying out Design Science Research Methodology .....	46
2.5	RESEARCH ETHICS .....	48
2.6	SUMMARY .....	49
<b>3</b>	<b>LITERATURE REVIEW: EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK.....</b>	<b>51</b>
3.1	INTRODUCTION.....	51
3.2	OVERVIEW OF CHAPTER 3.....	52
3.3	SYSTEMATIC LITERATURE REVIEW.....	53
3.3.1	Eight major steps in conducting a systematic literature review .....	54
3.3.2	Academic databases searched.....	55
3.3.3	Searching the literature.....	55
3.3.4	Inclusion and exclusion criteria.....	56
3.3.5	Literature search results .....	57
3.3.6	Data screening .....	57
3.3.7	Data analysis and selection .....	60
3.4	CYBER SECURITY AWARENESS.....	62
3.4.1	Relationship between information security and cyber security .....	62
3.4.2	Overview of cyber security awareness .....	64
3.4.3	Cyber security awareness in South Africa .....	66
3.4.4	Discussion of studies in Table 3-3.....	68



3.4.5	Cyber security awareness models and frameworks .....	68
3.4.6	Discussion of studies in Table 3-5 .....	73
3.5	COMPONENTS FOR CYBER SECURITY AWARENESS FRAMEWORK .....	78
3.5.1	Clearly articulate goals and objectives .....	80
3.5.2	Appoint a dedicated team .....	81
3.5.3	Identify current training needs .....	82
3.5.4	Obtain support in the form of partnerships.....	83
3.5.5	Identify target audiences.....	85
3.5.6	Define topics to cover and their delivery methods .....	85
3.5.7	Establish a cyber security policy .....	87
3.5.8	Develop a strategy for implementation .....	88
3.5.9	Design an awareness and training strategy.....	89
3.5.10	Define evaluation methods.....	90
3.5.11	Ten components of a cyber security awareness framework.....	91
3.6	SUMMARY.....	92
<b>4</b>	<b>THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY AWARENESS FOR SOUTH AFRICAN SMMEs.....</b>	<b>95</b>
4.1	INTRODUCTION.....	95
4.2	OVERVIEW OF CHAPTER 4.....	96
4.3	BUSINESS CHARACTERISTICS OF SOUTH AFRICAN SMMEs.....	96

4.3.1	Defining SMMEs.....	96
4.3.2	Phases of SMME development .....	97
4.3.3	Characteristics of SMMEs .....	100
4.3.4	Importance of SMMEs in a country.....	101
4.3.5	Information technology dependency.....	102
4.3.6	Challenges faced by SMMEs.....	103
4.4	THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK .....	107
4.4.1	Introduction.....	107
4.4.2	Constructing the intermediate Csa4Smme {RSA} framework.....	109
4.4.3	Four high-level stages of the NIST framework.....	110
4.4.4	Five layers of the cyber security awareness and education framework...	111
4.4.5	The intermediate Csa4Smme {RSA} framework.....	156
4.5	SUMMARY.....	158
<b>5</b>	<b>VALIDATION OF THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK..</b>	<b>160</b>
5.1	INTRODUCTION.....	160
5.2	OVERVIEW OF CHAPTER 5.....	161
5.3	DEMONSTRATION AND EVALUATION IN DESIGN SCIENCE RESEARCH METHODOLOGY .....	161
5.4	DEFINING AN EXPERT.....	162
5.4.1	Defining validation phase.....	162

5.4.2	Selection process .....	163
5.5	INTERVIEW PROCESS.....	166
5.5.1	Interview guide .....	167
5.5.2	Interview questions.....	168
5.5.3	Stages of validating the framework.....	169
5.6	FINDINGS FROM INTERVIEWS .....	170
5.6.1	Components of the strategic layer .....	173
5.6.2	Components of the tactical layer .....	175
5.6.3	Components of the preparation layer .....	177
5.6.4	Components of the delivery layer .....	179
5.6.5	Components of the monitoring layer.....	180
5.6.6	Comments and suggestions .....	182
5.7	A FRAMEWORK FOR CYBER SECURITY AWARENESS IN SMALL, MEDIUM AND MICRO ENTERPRISES (SMMEs).....	186
5.8	SUMMARY.....	189
<b>6</b>	<b>FINAL DISCUSSION AND CONCLUSION .....</b>	<b>191</b>
6.1	INTRODUCTION.....	191
6.2	OVERVIEW OF CHAPTER 6.....	191
6.3	REVIEW OF THE RESEARCH PROBLEM .....	191
6.4	REFLECTION ON RESEARCH QUESTIONS .....	192

6.5	SUMMARY OF THE RESEARCH DESIGN .....	195
6.6	SUMMARY OF RESEARCH CHAPTERS .....	197
6.7	RESEARCH CONTRIBUTION .....	198
6.8	LIMITATIONS.....	199
6.9	FUTURE RESEARCH.....	199
6.10	CONCLUSION .....	200
<b>7</b>	<b>REFERENCES.....</b>	<b>201</b>
<b>8</b>	<b>LIST OF APPENDICES .....</b>	<b>226</b>
8.1	APPENDIX A: TABLES .....	226
8.2	APPENDIX B: NO HUMANS INVOLVED (ETHICAL APPROVAL) .....	245
8.3	APPENDIX C: HUMANS INVOLVED (ETHICAL APPROVAL) .....	247
8.4	APPENDIX D: PERMISSION LETTERS .....	250
8.5	APPENDIX E: CONSENT FORM.....	252
8.6	APPENDIX F: PARTICIPANT INFORMATION SHEET .....	253
8.7	APPENDIX G: LANGUAGE EDITING CERTIFICATE .....	256

## LIST OF FIGURES

Figure 1-1: Design Science Research Methodology Process (Adapted from Peffers et al., 2007).....	19
Figure 1-2: Summarised DSRM process applied in the study .....	21
Figure 2-1: Phases of the study: The intermediate Csa4Smmes {RSA} framework.....	31
Figure 2-2: The principle of hermeneutic circle, as adapted from Boell and Cecez-Kecmanovic (2010) .....	37
Figure 2-3: A research framework (March & Smith, 1995) .....	39
Figure 2-4: DSRM process and possible research entry points (Peffers et al., 2007) ...	41
Figure 3-1: DSRM Process - Phase 1: Literature study.....	52
Figure 3-2: Flow chart based on search phases for literature on cyber security awareness for SMMEs .....	58
Figure 3-3: Relationship between information security, ICT security and cyber security (Von Solms & Van Niekerk, 2013).....	63
Figure 3-4: Components of a cyber security awareness framework for SMMEs (Lejaka et al., 2019) .....	92
Figure 4-1: DSRM Process - Phase 2: The development of the intermediate Csa4Smmes {RSA} framework.....	95
Figure 4-2: Five phases of SMME development (Lewis & Churchill, 1983).....	97
Figure 4-3: Five layers of the intermediate Csa4Smmes {RSA} framework (Kortjan & Von Solms, 2014).....	111
Figure 4-4: PDCA and PDCA integration in the intermediate Csa4Smmes {RSA} framework for SMMEs.....	113
Figure 4-5: PDCA cycle (ISO/IEC 27000, 2009) .....	114
Figure 4-6: Resource components required for the intermediate Csa4Smmes {RSA} framework for SMMEs.....	115

Figure 4-7: The strategic layer of the intermediate Csa4Smmes {RSA} framework. ...	118
Figure 4-8: The tactical layer of the intermediate Csa4Smmes {RSA} framework .....	128
Figure 4-9: The preparation layer of the intermediate Csa4Smmes {RSA} framework. .....	137
Figure 4-10: The delivery layer of the intermediate Csa4Smmes {RSA} framework ...	144
Figure 4-11: The monitoring layer of the intermediate Csa4Smmes {RSA} framework	151
Figure 4-12: The intermediate Csa4Smmes {RSA} framework .....	157
Figure 5-1: DSRM Process - Phase 3: The validation of the intermediate Csa4Smmes {RSA} framework.....	160
Figure 5-2: Components of the strategic layer - thematic network diagram .....	173
Figure 5-3: Components of the tactical layer - thematic network diagram.....	175
Figure 5-4: Components of the preparation layer - thematic network diagram.....	177
Figure 5-5: Components of the delivery layer - thematic network diagram.....	179
Figure 5-6: Components of the monitoring layer - thematic network diagram .....	181
Figure 5-7: Demonstration of the intermediate Csa4Smmes {RSA} framework - thematic network diagram.....	182
Figure 5-8: Validation of the intermediate Csa4Smmes {RSA} framework - thematic network diagram.....	183
Figure 5-9: Integration for the intermediate Csa4Smmes {RSA} framework - thematic network diagram.....	184
Figure 5-10: A framework for cyber security awareness in SMMEs .....	188

## LIST OF TABLES

Table 2-1: Philosophical assumptions of the four research paradigms (Adebesin, 2011; Terre-Blanche et al., 2006) .....	27
Table 2-2: Deductive and inductive research approach characteristics (Bryman & Bell, 2015; Buthelezi, 2017; Creswell, 2014; Gcaza, 2017; Hesse-Biber & Leavy, 2010; Robson, 2002; Saunders et al., 2007; Silverman, 2013).....	29
Table 2-3: Data collection techniques (Creswell, 2014; Kumar, 2011) .....	33
Table 2-4: Guidelines for carrying out design science research methodology .....	47
Table 3-1: Databases searched .....	57
Table 3-2: Research categories .....	60
Table 3-3: Matrix analysis (awareness scope) of studies measuring cyber or information security awareness levels (from Category 1 of Table 3-2) .....	67
Table 3-4: Existing cyber security awareness models and frameworks (from Categories 3 and 4 of Table 3-2).....	69
Table 3-5: Matrix analysis of cyber security awareness models and frameworks identified .....	71
Table 3-6: Summary of the key aspects for goals and objectives .....	80
Table 3-7: Summary of the key aspects for appointing a dedicated team .....	81
Table 3-8: Summary of the key aspects for identifying existing training needs .....	83
Table 3-9: Summary of the key aspects for forming partnerships .....	84
Table 3-10: Summary of the key aspects for identifying target audiences .....	85
Table 3-11: Summary of the key aspects for defining topics to be covered .....	86
Table 3-12: Summary of the key aspects for establishing a cyber security policy .....	87
Table 3-13: Summary of the key aspects for developing a strategy for implementation .....	88
Table 3-14: Summary of the key aspects for designing strategies for awareness and training .....	89

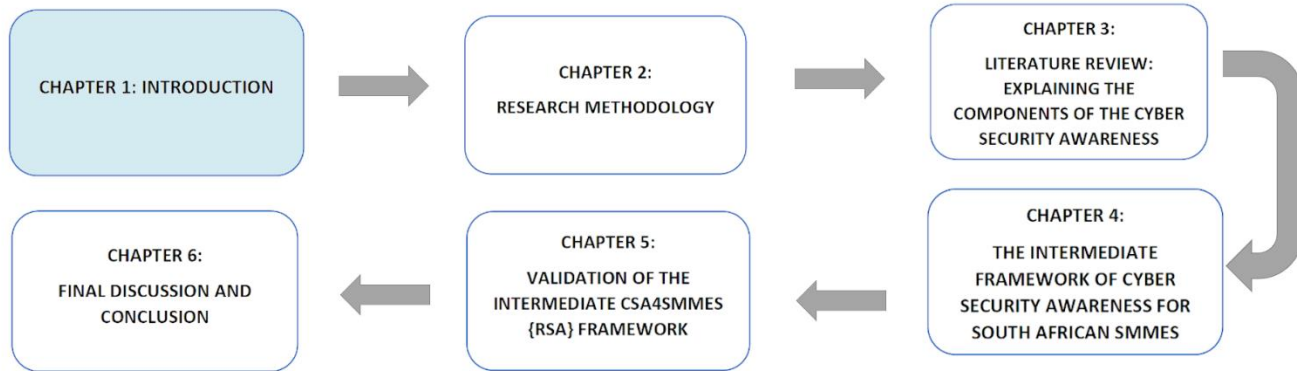
Table 3-15: Summary of the key aspects for defining evaluation methods .....	90
Table 4-1: Key symbols for relevant models and frameworks used to identify components of the intermediate Csa4Smmes {RSA} framework.....	112
Table 4-2: The relationship between the responsible party and corresponding role in the strategic layer of the intermediate Csa4Smmes {RSA} framework .....	118
Table 4-3: Executive roles of components in the strategic layer of the intermediate Csa4Smmes {RSA} framework .....	126
Table 4-4: The relationship between the responsible party and corresponding role in the tactical layer of the intermediate Csa4Smmes {RSA} framework.....	128
Table 4-5: Executive roles for components in the tactical layer of the intermediate Csa4Smmes {RSA} framework .....	135
Table 4-6: The relationship between the responsible party and corresponding role in the preparation layer of the intermediate Csa4Smmes {RSA} framework.....	137
Table 4-7: Executive roles for components in the preparation layer of the intermediate Csa4Smmes {RSA} framework .....	143
Table 4-8: The relationship between the responsible party and corresponding role in the delivery layer of the intermediate Csa4Smmes {RSA} framework .....	145
Table 4-9: Executive roles of components in the delivery layer of the intermediate Csa4Smmes {RSA} framework .....	149
Table 4-10: The relationship between the responsible party and corresponding role in the monitoring layer of the intermediate Csa4Smmes {RSA} framework .....	151
Table 4-11: Executive roles of components in the monitoring layer of the intermediate Csa4Smmes {RSA} framework .....	155
Table 5-1: Background information about expert reviewers .....	165
Table 5-2: Validation timelines .....	170
Table 5-3: List of components added, removed or modified to form the Csa4Smmes {RSA} framework.....	187



## PUBLICATIONS

Lejaka, T. K., Da Veiga, A., & Looock, M. (2019). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. *2019 Conference on Information Communications Technology and Society, ICTAS 2019*.<https://doi.org/10.1109/ICTAS.2019.8703609>

# CHAPTER 1: INTRODUCTION



<b>CHAPTER 1: INTRODUCTION</b>	1.1	OVERVIEW OF CHAPTER 1	1.2	INTRODUCTION
	1.3	BACKGROUND	1.4	PROBLEM STATEMENT AND RESEARCH QUESTIONS
	1.5	RESEARCH METHODOLOGY	1.6	ETHICAL CONSIDERATIONS
	1.7	OVERVIEW OF CHAPTERS	1.8	SUMMARY

# **1 INTRODUCTION**

## **1.1 OVERVIEW OF CHAPTER 1**

This study aims to develop a framework for cyber security awareness for South African SMMEs (Csa4Smmes {RSA} framework). This chapter begins with an introduction and background of the study (Section 1.2 and Section 1.3 respectively). Then follows a discussion regarding the problem statement and research questions of the research study (Section 1.4). A brief discussion regarding the research methodology is described in Section 1.5, with another brief discussion regarding the ethical considerations provided in Section 1.6. An overview of the research chapters is provided in Section 1.7.

## **1.2 INTRODUCTION**

In South Africa, there is a rapid increase in cyber attacks intended for organisations regardless of size and industry (IRMSA, 2017). According to the survey report by PricewaterhouseCoopers (PwC), cyber attacks have emerged to be a vigorous threat to businesses regardless of size and industry (PwC, 2020). Small, medium and micro enterprises (SMMEs) are targets of cyber attacks (Symantec, 2017). However, SMMEs do not have adequate information technology (IT) skills and financial support to prevent prevalent cyber threats. Organisations, regardless of size and industry, should set up a collection of tools to protect the networks, computers, programs and other assets owned by users and organisations against cyber attacks (Dlamini & Modise, 2012). Cyber security awareness (CSA) plays a significant role in enhancing the level of awareness of cyber security. In addition, cyber security awareness aims to provide support for users to be conscious of and dedicated to organisations' cyber security policies regardless of job designation (Siponen, 2000).

## **1.3 BACKGROUND**

According to the seventh South African Edition Global Economic Crime Survey by PwC, many organisations are still not effectively prepared to prevent cybercrimes (PwC, 2020). The survey stated that organisations have an inadequate understanding of cyber threats

and risks. Furthermore, the survey indicates that only 35 percent of organisations have a cyber incident response plan, denoting that many organisations are not prepared to deal with cyber attacks. Cyber attacks are directed at businesses of all sizes; however, SMMEs are impacted most (Symantec, 2017). According to PwC (2020), 31 percent of South African organisations have been victims of cybercrime even though other incidences are not reported. According to the Symantec Internet Security Threat Report (2019), the percentage of cyber attacks on SMMEs has been increasing compared to previous years (Symantec, 2019). The Institute of Risk Management South Africa (IRMSA) has stated that cyber attacks are one of the major risks affecting the economy of the country (IRMSA, 2019). During 2015, Symantec blocked 43 percent of targeted spear-phishing attacks intended for SMMEs. In conclusion, SMMEs are increasingly becoming one of the main targets for cyber criminals (Von Solms, 2015).

In the next sub section, key concepts relating to cyber security awareness will be discussed in detail. Therefore, it is important to understand cyberspace in terms of opportunities and challenges it brings forth.

### **1.3.1 What is cyberspace?**

Cyberspace can be defined as a way to communicate, access and interact on social networking sites, to make financial transactions, to search for information and to access entertainment platforms (Gheorghica & Croitoru, 2016). In addition, users, including SMMEs, can access a variety of global opportunities through cyberspace. However, cyberspace is considered an unregulated and dangerous platform (Kritzinger, Bada, & Nurse, 2017) and there are numerous risks associated with it. In addition, cyberspace allows users to access a variety of technologies, including the internet, which allows them to access different kinds of online services, although there are risks associated with them. Countless users of the internet are not alert about the dangers within cyberspace (Adelola, Dawson & Batmaz, 2015; Kritzinger et al., 2017; LeFebvre, 2012; Sarathchandra, Haltinner, & Lichtenberg, 2016).

The core element influencing changes in cyber threats is mainly associated with the increased universal population accessing the internet (Rahim, Hamid, Mat Kiah,

Shamshirband, & Furnell, 2015). The internet is the most commonly influential factor that contributes to the vulnerability of people and organisations against external attacks (Iguer, Medromi, Sayouti, Elhasnaoui, & Faris, 2014). Internet users are spending more time accessing social networks and these users are exposing themselves to diverse risks (De Bruijn & Janssen, 2017).

Cyber criminals often exploit developing countries like South Africa with weak security controls to target developed countries (partners) with the intention of gaining access to large international organisations (Mbelli & Dwolatzky, 2016). Similarly, cyber attackers target SMMEs to gain access to these organisations (Ngalonkulu, 2018). Therefore, SMMEs are directly involved in the creation of a secure cyber security infrastructure of a country. Cyber security is a worldwide occurrence representing multi-faceted social and technical challenges intended for governments but also demanding the public sector to participate (De Bruijn & Janssen, 2017). Furthermore, cyber security is costly and it is considered one of the most vital challenges encountered by governments because having an all-inclusive security protection system is not possible (De Bruijn & Janssen, 2017).

### **1.3.2 Cyber security, a global concern**

Cyber security has emerged to be a global concern for all countries because both developing and developed countries are in formation to establish or enhance methods to be utilised to deal with cyber issues (Iguer et al., 2014). Countries must set up cyber security systems to deal with cyber issues that are spread globally. Therefore, this subsection provides a discussion about global cyber related attacks.

The WannaCry ransomware attack is one of the largest cyber attacks which has affected personal computers in companies around the world (Sherr, 2017). The WannaCry ransomware has affected computer systems globally, including but not limited to the United States of America, Russia, China and the United Kingdom. The WannaCry attack locks and encrypts all data on the computer systems that have been affected. Then ransom payment in the form of an untraceable digital currency called Bitcoin (a method of payment whereby payments can be initiated without involving banking systems) is demanded from affected users to recover and retrieve their data (Hern, 2017). In addition,

the WannaCry ransomware has affected Microsoft Windows-based computers by exploiting a vulnerability on the operating system. However, after the incident Microsoft has released a software update to patch the vulnerability of the operating system.

Yet, another encrypting ransomware attack called Petya ransomware has also affected Microsoft Windows-based systems. Ransomware like WannaCry uses the EternalBlue exploit as one of the means to affect and spread itself within computer systems within the organisation (Solon & Hern, 2017). Petya is different from other typical ransomware attack because it locks and encrypts all data in computer systems (Symantec, 2017). In addition, it modifies and encrypts the master boot record (MBR) to hijack the normal loading procedure of the infected computing device when rebooting. Petya has also affected many organisations globally, including Ukraine, Spain, Russia, the United States of America and South Africa, and ransom payment is required to be paid using Bitcoin.

In another case, an internet infrastructure company called Cloudflare, which provides security services for a multitude of websites (Newman, 2017), has discovered a bug called Cloudbleed (Holland, 2017). In 2017, Cloudbleed was identified as the most recent internet bug that exposed private information of users within cyberspace (Popular Mechanics, 2017). Cloudbleed was responsible for leaking confidential information such as usernames, passwords, application programming interface (API) keys, sensitive cookies, message contents, and other data (Newman, 2017). Despite personal and confidential information being exposed, Cloudflare managed to fix the bug to improve the security and protect data from websites.

In August 2013, Yahoo experienced a historic data breach which affected all existing user accounts, while personal and confidential information was breached; however, financial information was not breached (Larson, 2017). The following year, around 500 million Yahoo users were affected again, and this breach was believed to be a separate data breach from the 2013 breach (Larson, 2017). The stolen data are then sold on the dark web which is a platform only accessible through specified software (USAToday, 2017).

Facebook Inc. also recorded its biggest data breach in more than five years. Facebook reported that an advertising data firm called Cambridge Analytica helped Donald Trump

to win the United States presidency by retrieving and retaining information on millions of Facebook users without their permission (Elgot & Hern, 2018). Cambridge Analytica collected tons of information about Facebook profiles to influence decision making when voting. The harvested data were misused, and government officials from the United States and Europe demanded solutions from Facebook regarding the data leakage and privacy breach (Bloomberg, 2018). Therefore, cyber security is a global concern, meaning it affects individuals, companies and countries regardless of nationality. However, it is important for South Africa to implement measures to mitigate cyber attacks.

### **1.3.3 Cyber security in South Africa, a developing country**

South Africa has also suffered its largest data breach when approximately 60 million South Africans' personal data, including unique identity numbers of living citizens, deceased citizens and citizens living overseas were leaked (Venktesh, 2017). Recently, in South Africa, a credit bureau called Experian has suffered a massive data breach that exposed information of 24 million individual South Africans and 800 000 businesses (eNCA, 2020). The massive data leak included confidential information such as personal information, contact information and employment details.

In another incident, the website of the local movie theatre Ster-Kinekor bookings leaked around seven million users' data. It was stated that there was a vulnerability in Ster-Kinekor's back-end system of the old website. It allowed unauthorised people to access confidential data which included personal details, contact details, addresses and the passwords of all these users (Venktesh, 2017). Furthermore, the Ster-Kinekor API gained access to data from the database which provided details of all users in the database, including their passwords stored as plain text (Vermeulen, 2017b).

Cyber security needs to be addressed globally regardless of the trading industry. South African financial institutions, including banks, were also affected by cyber outbreaks. First National Bank (FNB) and MTN were impacted in the SIM swop scam which stole hundreds of thousands of rands from customers (Van Zyl, 2016). MTN was unable to prevent illegal SIM swop processes which permitted attackers to illegally use SIM cards to steal money from client accounts. According to the article, FNB acknowledged that

phishing has always been a problematical method of scamming people of their money (News24 Wire, 2016).

ABSA and Vodacom were also impacted by the SIM swop scam. The attackers managed to steal money from ABSA clients by conducting an illegal Vodacom SIM swop (Staff Writer, 2017). The attackers gained access to the banking accounts and used the illegal SIM cards to authenticate transactions. However, ABSA stated that it had no control regarding online banking fraud because such attacks could only be conducted through phishing attacks and SIM swop fraud (Staff Writer, 2017). South African banks (including FNB and ABSA) published phishing incidences on their official websites to help clients identify such attacks.

South Africa is considered a developing country (World Economic Forum, 2017). According to the research done by Stellenbosch University, South African SMMEs are found to be less innovative compared to SMMEs in developed countries (Bureau for Economic Research, 2016). Furthermore, IRMSA (2017) identified lack of innovation as one of the top South African industrial risks. One of the problematic factors of doing business in South Africa is insufficient capacity to innovate (World Economic Forum, 2017). Therefore, cyber security awareness for SMMEs should be tailored because South African SMMEs are unique. SMMEs in developing countries do not have adequate access to the latest technologies compared to SMMEs in developed countries (World Economic Forum, 2017). Consequently, South African SMMEs might be incompetent in utilising the latest cyber security technological tools to mitigate cyber threats.

Furthermore, Mark Heyink states that government has been unsuccessful in achieving a constitutional mandate regarding the employment of cyber inspectors (Heyink, 2015). The article states that the assurance by governments towards information security and cyber security has been a challenging battle. The South African Cyber Security Hub has been established by the Department of Telecommunications and Postal Services to serve as a focal point for collaboration between government, industry and the public towards cyber security related incidents in South Africa (Cybersecurity Hub, 2016).



Currently in South Africa, initiatives such as the Bill for Cybercrimes and Cyber Security have been established to deal with cyber issues (Department of Justice and Constitutional Development, 2017). This Bill primarily aims to promote cyber security in the private sector to establish a support structure that promotes and builds capacity towards cyber security. Furthermore, the Bill aims to establish a 24/7 Point of Contact to construct faults and enforce penalties which have a bearing on cybercrime within the country. The Bill aims to build a cyber security culture and promote cyber security for South African citizens. Therefore, South African SMMEs should be provided with knowledge regarding cyber security so that they will be able to protect employees and customers against cyber threats. The Bill also aims to enforce obligations for organisations to contribute to the investigation and reporting of cybercrimes within the country.

As stated in the Bill, access to information about cyber security occurrences within the country is limited (Department of Justice and Constitutional Development, 2017). Information sharing concerning cyber security might be caused by the fact that some cyber incidents are not reported (PwC, 2016). To address that, cyber security awareness assists with providing SMMEs with adequate knowledge related to cyber security. Therefore, it is mandatory for South African SMMEs to have access to information regarding current occurrences linked to the latest cyber threats and vulnerabilities to enhance the level of awareness within SMMEs.

The Bill states that information sharing ensures that acceptable measures are implemented against cybercrimes. Currently in South Africa, there is no coherent and structured approach to deal with cybercrimes because both the private and public sectors have insufficient capacity to deal with issues regarding cyber security (Department of Justice and Constitutional Development, 2017). As stated in the Bill, the National Cyber Security Policy Framework (NCPF) has been developed to provide measures for addressing national security and preventing cybercrimes within cyberspace. The government gradually promulgated the proposed Bill (Sutherland, 2017), however, recently the President signed the Bill into a law (Moyo, 2021) and as of 1 July 2021, most sections of POPI Act are effective. Therefore, SMMEs should have access to cyber security to ensure that they are aware of acceptable measures required to combat

cybercrimes. Furthermore, providing cyber security awareness within SMMEs will raise awareness for employees and employers so that they can carry out secured activities within the organisations.

The South African parliament has approved the Protection of Personal Information (POPI) Act, 4 of 2013, which requires all companies, including SMMEs, to have adequate security to protect personal information of individuals (Von Solms, 2015). However, the Code of Conduct per industry, including SMMEs, has not be developed yet by the regulator (News24, 2020). The POPI Act of 2013 aims to align South Africa with global laws. The POPI Act aims to promote the safeguarding of personal information administered and handled by the public and private sectors. The overall enforcement of the POPI Act of 2013 by government will provide an opportunity to protect the use of personal information. The Act enforces that all South African institutions (including SMMEs) who gather, hold, distribute and use personal information of consumers must be responsible and account for any data breach that might happen within the institute.

#### **1.3.4 Current state of South Africa towards information communication technology**

Currently in South Africa, numerous activities such as studying, communicating, dating, shopping, banking and more are conducted online. These activities were enabled through the implementation of information communication technology (ICT) services, including access to mobile computing, the internet, online financial transactions, hardware, software, cloud computing, and any other ICT-related services. In South Africa, there are business incubators from which SMMEs can benefit. These incubators provide SMMEs with sustainable and essential entrepreneurial support to minimise the rate of failure (Crampton, 2019). In addition, business incubators can provide SMMEs with access to ICT-related services which will enable SMMEs to be innovative.

SMMEs in South African can utilise ICT services available to them such as free internet solutions. The City of Tshwane indicates on their website that Tshwane's free Wi-Fi (TshWi-Fi) service has delivered free accessible internet by utilising around 780 hotspots implemented within the City of Tshwane (City of Tshwane, n.d.). Technology has

advantaged communities and cities by transforming learning institutions, health centres and libraries into hotspots. In addition, the City of Tshwane indicates that, since the initiation of the TshWi-Fi project, over and above 1.6 million unique computing devices have accessed the network. In addition, TshWi-Fi network is emphasised as the largest Wi-Fi network in Africa (City of Tshwane, n.d.).

Furthermore, the City of Tshwane is the largest municipality on the African continent and third largest worldwide (Geerdts et al., 2016). Compared with other South African municipalities, the City of Tshwane provides the most innovative wireless network in the country in relation to scalability and impact on citizens. Furthermore, the City of Tshwane provides economical support by providing an increased broadband to the public, aiming to grow the economy, increase commercials and intensify financial activities within the city (Geerdts et al., 2016).

In addition, South African towns with existing or proposed initiatives for access to free Wi-Fi include Knysna, Stellenbosch, the City of Tshwane, the City of Johannesburg, Ekurhuleni, the City of Cape Town, Durban, Gqeberha (formerly known as Port Elizabeth) and Klerksdorp (Geerdts et al., 2016). South African SMMEs have access to such wireless networks which come along with their related cyber threats because wireless networks are prone to several attacks (Mekhazniaa & Zidania, 2015). Furthermore, wireless networks are usually sensitive to eavesdropping. Therefore, it is mandatory for all data transmitted through network nodes to be encrypted permanently to prevent unauthorised users from gaining access to the content.

Wireless networks are vulnerable to several types of attacks including denial of service (DoS) attacks, node takeovers, traffic analyses, and other attacks. However, SMMEs in developing countries do not have adequate access to the latest technologies compared to SMMEs in developed countries (World Economic Forum, 2017). Therefore, SMMEs will not be able to protect themselves against cyber attacks delivered through the connection on wireless networks that are implemented and accessible across South Africa. These unaware users (SMMEs) are well-known for connecting into open and unsafe Wi-Fi hotspots (Geerdts, Gillwald, Calandro, Chair, Moyo, & Rademan, 2016;

Pinzon & Nachreiner, 2008). Through that process, cyber attackers can access confidential information (including login details, organisational data stored on the devices) and personal information of users (including their passwords). Therefore, the attackers will use that collected data to target a specific SMME. Since the Bill for Cybercrimes and Cyber Security is partially in place, guidance for SMMEs is required to mitigate successful cyber security attacks that are human related.

### **1.3.5 The importance of cyber security awareness**

Cyber security awareness is important and can be used to reduce cyber threats because many studies across the world use awareness to mitigate cyber threats (Grobler, Flowerday, Von Solms, & Venter, 2011a; Labuschagne & Eloff, 2012; Mbelli & Dwolatzky, 2016; Muhirwe, 2016; Parsons, Calic, Pattinson, Butavicius, McCormac, & Zwaans, 2017). Cyber security awareness helps in securing cyberspace and in providing support to promote an envisaged cyber security culture (Kortjan & Von Solms, 2014). The purpose of awareness is to prepare internet users to have emergency plans in place against cyber attacks (Rahim et al., 2015).

Furthermore, cyber security awareness has been demonstrated to be an effective approach in reducing the threat of cyber attacks associated with internet users (Muhirwe, 2016). Cyber security awareness is mainly designed in an attempt to prevent naive internet users from becoming targets of cyber attacks (Grobler, Van Vuuren, & Zaaiman, 2011b). This kind of awareness is vital to reduce cyber security threats that occur due to human-related vulnerabilities (Abawajy, 2014). Cyber security awareness is essential because it enables society to improve its cyber security practices while conducting activities within cyberspace (Alotaibi, Furnell, Stengel, & Papadaki, 2016).

The establishment of cyber security awareness is the most preeminent method to fight cybercrimes (Alotaibi et al., 2016). It is significant for people to have elementary knowledge about cyber security attacks and vulnerabilities (Tirumala, Sarrafzadeh, & Pang, 2019). When delivering cyber security awareness, the message must effectively reach people of all ages. It is also significant to ensure that knowledge about cyber security is transferred in such a way that the target audience receives acceptable

attention (Rahim et al., 2015). Therefore, it is important to provide cyber security awareness to instil knowledge about cyber security within SMMEs.

### **1.3.6 Audience analysis for cyber security awareness**

It is important to categorise users when conducting cyber security awareness to ensure that the relevant message is conveyed to the appropriate target audience. Numerous training methods are unsuccessful because they do not allow users to reflect and apply security concepts (Cone, Irvine, Thompson, & Nguyen, 2007). When conducting cyber security awareness, it is important to distinguish between multiple audiences which require different messages (De Bruijn & Janssen, 2017) because cyber criminals frequently target uninformed individuals with no or limited knowledge on how to recognise cyber attacks. In addition, when conducting cyber security awareness, it is important to analyse the target audience and consider the integration of multiple languages to avoid having skewed data due to language barriers (Grobler et al., 2011a), because in South Africa there are 11 official languages. Therefore, it is significant to provide tailored cyber security awareness with the integration of multiple languages, since SMMEs have diverse backgrounds.

### **1.3.7 Motivation for cyber security awareness**

Technical measures independently are inadequate to solve critical IT security difficulties (Arachchilage & Love, 2014; Ramírez, 2017). Therefore, combining the usage of technical measures together with awareness might help to mitigate threats (Abawajy, 2014). Adelola et al. (2015) indicate that different materials can be developed to convey an appropriate message that is relevant to an audience's needs and knowledge. Furthermore, cyber threats can be mitigated by providing tailored awareness for all internet users within SMMEs (Alotaibi et al., 2016).

### **1.3.8 People are the weakest link**

Several studies state that people are the weakest link within the cyber security chain (Abawajy, 2014; Anwar, He, Ash, Yuan, Li, & Xu, 2017; De Bruijn & Janssen, 2017). Professionals also agree that people are the weakest link regarding the protection of

information systems within organisations. People are frequently denoted as the first line of defence against several security threats (Parsons et al., 2017) because human error generally plays a role in cyber security breaches.

Yet, the best valuable technology-based security solutions not accompanied by awareness cannot deliver complete security which is required to protect organisational assets against prevalent threats (Abawajy, 2014). Cyber security breaches are widespread in organisations of all types and these breaches are frequently sanctioned by human errors (Anwar et al., 2017). These breaches can cause issues related to both financial and non-financial losses within a company and for its clients (Mbelli & Dwolatzky, 2016). Therefore, individuals within SMMEs should be exposed to cyber security awareness in order to mitigate cyber attacks that are linked to human errors because SMMEs are experiencing numerous challenges as discussed in the next sub-section.

### **1.3.9 Challenges faced by SMMEs**

In South Africa, cyber risk is declared the top concern for all businesses (Fin24Tech, 2018). However, financial resources are regularly identified as limitations to implement effective cyber security mechanisms (Kent, Tanner, & Kabanda, 2016). Many SMMEs cannot afford to implement an effective internal cyber security plan (Von Solms, 2015). However, unsecured actions of SMMEs can critically influence the overall cyber security of the country. Several South African SMMEs do not have access to cyber security support structures. As stated on the Small Business Development Agency (SEDA) website, SEDA aims to empower and support SMMEs; however, there is no indication of providing cyber security support for SMMEs (Small Business Development Agency, n.d.).

All nations constantly try to ease the effect of cyber terrorism and strive to enhance their resilience to cyber threats and incidents (Iguer et al., 2014). Therefore, in South Africa, challenges faced by SMMEs, which includes limited or no cyber security knowledge, must be addressed. (Kent et al., 2016). However, a detailed discussion regarding SMME characteristics and challenges will be covered in Section 4.3.

In the next section, a brief discussion concerning the problem statement and the research questions is presented.

#### **1.4 PROBLEM STATEMENT AND RESEARCH QUESTIONS**

Recently in South Africa, there has been a rapid increase in cyber attacks intended for organisations regardless of size and industry (Creamer Media, 2020; Fin24Tech, 2018; IRMSA, 2017; IT News Africa, 2017). Despite the rapid increase in cyber threats SMMEs do not always pay attention to cyber security issues (Kent et al., 2016). Therefore, the South African cyber security infrastructure could be compromised through numerous insecure activities conveyed by SMMEs.

Many SMMEs cannot afford adequate cyber security controls due to unstable financial resources (OECD, 2015). Most South African SMMEs do not have sufficient access to finances, as they generate deprived profitability (Mansfield-Devine, 2016). Hence, it is significant for SMMEs to have access to cyber security awareness programmes that are relevant and customised for them because they are unique in terms of phases of development, characteristics and challenges faced.

A cyber security awareness enables SMMEs to effectively reduce the threat of cyber attacks associated with internet users (Muhirwe, 2016) because people are the weakest link in securing the cyber security infrastructure (Anwar et al., 2017; Arachchilage & Love, 2014). Kortjan and Von Solms (2014) point out that many South African internet users lack awareness of cyber security. These users are ignorant and at risk of having their personal and confidential information being exploited by unauthorised parties (Kortjan & Von Solms, 2014). People, regardless of their role in SMMEs, are easy targets for exploitation because of their insecure activities, increased cyber threats and lack of cyber security awareness within SMMEs (Kent et al., 2016).

SMMEs contribute to the economy of the country and most importantly create employment opportunities for citizens (Kent et al., 2016; Paulsen, 2016; Statistics South Africa, 2017). In South Africa, there is an increased number of SMMEs (Small Business Development Agency, 2019; Statistics South Africa, 2017) and for that reason the South

African cyber security infrastructure is prone to cyber attacks due to unprotected activities conducted by multitudes of SMMEs within cyberspace.

The main research problem is that cyber attacks are directed at businesses of all sizes, however, SMMEs are impacted the most (Symantec, 2017). In addition, a large number of South African SMMEs are still not effectively prepared to prevent cybercrimes (PwC, 2016). PwC (2016) states that organisations, including SMMEs, have insufficient knowledge concerning cyber threats and risks. According to Amankwa, Loock, & Kritzinger (2016), SMMEs have limited resources and a semi-structured IT setup. It is unusual to find cyber security professionals occupying senior management positions within SMMEs compared to large organisations (Amankwa et al., 2016). Also, many SMMEs do not have sufficient cyber security-related resources compared to large organisations. In South Africa, like in other developing countries, numerous organisations have been victims of cybercrime, however, other incidences are not being reported.

The South African cyber security infrastructure is exposed to cyber attacks due to insecure activities conducted by multitudes of SMMEs. However, the South African government is experiencing challenges in protecting the national cyber security infrastructure, because they gradually promulgated the proposed Bill (Sutherland, 2017), however, recently the President signed the Bill into a law (Moyo, 2021). In addition, the South African government does not provide SMMEs with sufficient cyber security support which might enable SMMEs to address their cyber security issues internally.

South Africa must create initiatives to reduce cyber security threats and effectively improve cyber security in all areas, more precisely in SMMEs (Von Solms, 2015). Furthermore, the absence of government's cyber security awareness initiatives in this area (within the community of SMMEs) is causing severe cyber security-related problems in the country.

#### **1.4.1 Main research question**

To address the main research problem, the researcher formulated the following research question:



*What would constitute a cyber security awareness framework for South African SMMEs?*

#### **1.4.2 Sub-research questions**

To respond to the main research question, the following sub-research questions (SRQs) were formulated:

- SRQ1: What current studies measure cyber security awareness for SMMEs in South Africa?
- SRQ2: What existing cyber security awareness models or frameworks can be utilised for SMMEs?
- SRQ3: What components should be included in a cyber security awareness framework for SMMEs?
- SRQ4: What are the cyber security awareness needs within the South African community of SMMEs from a literature perspective?
- SRQ5: What would the intermediate Csa4Smmes {RSA} framework comprise for the South African community of SMMEs?

#### **1.4.3 Main research objective**

To assist South African SMMEs to reduce successful cyber attacks associated with human errors has led the researcher to formulate the main research objective:

*To develop a cyber security awareness framework for South African SMMEs.*

#### **1.4.4 Sub-objectives**

To meet the requirement for the main research objective has led the researcher to formulate the following sub-objectives:

- SRO1: To identify existing and current studies that measures cyber security awareness for SMMEs in South Africa.
- SRO2: To identify existing cyber security awareness models and frameworks that can be utilised for SMMEs.
- SRO3: To identify components of a cyber security awareness framework for SMMEs.
- SRO4: To identify factors related to characteristics and challenges faced by South African SMMEs.
- SRO5: To develop the intermediate Csa4Smmes {RSA} framework.

#### **1.4.5 Importance of the study**

The evolution of cybercrime in South Africa is rapidly becoming a serious financial challenge for organisations and ultimately the whole country. Developing nations such as South Africa focus more on increasing connectivity while overlooking the risks conveyed by such connectivity (Van Vuuren, Leenen, Phahlamohlaka, & Zaيمان, 2014). Currently, there is a need to create cyber security awareness for employees, employers, clients and suppliers in SMMEs because they have a direct impact on the cyber security infrastructure of the country. Furthermore, as stated by the Department of Telecommunications and Postal Services (2017), the country is vulnerable to cyber attacks and there is a common deficiency for cyber security professionals (Mbelli & Dwolatzky, 2016). The department has stated that there is a need to access and develop cyber security skills and awareness within the country because, if SMMEs do not have cyber security professionals working for them, they will not have the necessary skills required to mitigate the cyber risks.

This research focuses on contributing towards the cyber security culture for South African SMMEs because providing awareness for SMMEs might diminish the risk of successful cyber attacks associated with internet users (Muhirwe, 2016). In addition, the study contributes to the South African cyber security infrastructure because compromising

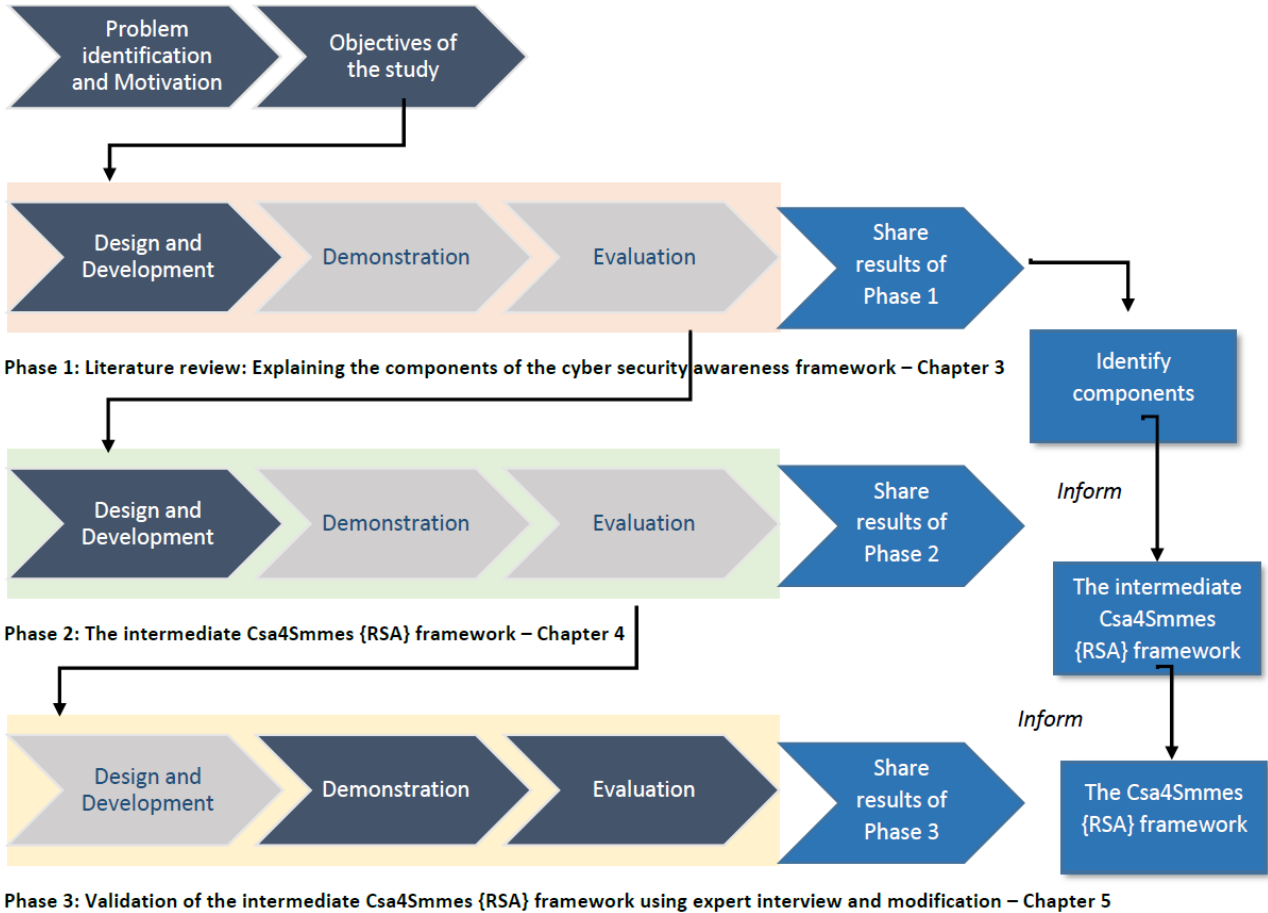
cyber security for SMMEs can have a crucial influence on the overall cyber security of the country (Von Solms, 2015).

The study provides support for SMMEs to be aware about cyber security which might help SMMEs in identifying and preventing basic cyber attacks (Kortjan & Von Solms, 2014). Cyber security awareness is vital for SMMEs because it provides them with essential and useful knowledge to make prudent decisions while conducting activities in cyberspace (Grobler et al., 2011a). Furthermore, Grobler et al. (2011a) state that it is essential to develop cyber security awareness using native languages which might improve the current level of awareness within SMMEs.

The proposed cyber security awareness for South African SMMEs (Csa4Smmes {RSA}) framework, will help SMMEs to improve their knowledge concerning cyber security and to prevent naive SMMEs from becoming victims of cyber attacks (Ramírez, 2017). This framework will provide awareness for SMMEs with the aim of supporting government in tackling the challenge of attaining comprehensive security protection for the country.

## **1.5 RESEARCH METHODOLOGY**

The research methodology is a procedure or technique to be followed in the research study. This study follows the Design Science Research Methodology (DSRM) approach. The study has adopted the DSRM process of Peffers, Tuunanen, Rothenberger and Chatterjee (2007). This section provides a graphical representation of the DSRM process which will be discussed further in Chapter 2. Figure 1-1 includes the representation of the discussion about the research objectives, problem statement and motivation for conducting this study (Chapter 1). The next sub-section will briefly discuss all phases as shown in Figure 1-1. In figure, all DSRM phases (phase 1 to phase 3) consist of an individual or a set of activities, whereby focal point is indicated by unshaded blocks.



**Figure 1-1: Design Science Research Methodology Process (Adapted from Peffers et al., 2007)**

The DSRM proposed by Peffers et al. (2007) describes the process to be followed – from problem definition and motivation through the development and validation of an artefact and the final dissemination of results. Therefore, this DSRM is most suitable and therefore it was carefully selected to address the purpose of this study. The DSRM process clarifies the research plan and outlines the structure of the study. This process comprises six stages (phases or activities), namely problem identification and motivation, objectives for a solution, design and development, demonstration, evaluation and communication. The DSRM phases, as depicted in Figure 1-1, consist of six activities and four possible research entry points. The six activities are:

- *Problem identification and motivation:* This activity is the initial phase where the researcher must specify the research problem and justify the value of a solution. The importance of motivating the solution is to ease the approval of the results and to simplify the researcher's knowledge of the problem (Peppers et al., 2007). This stage is also an entry point when the framework is a problem-centred initiation.
- *Definition of objectives of a solution:* In this activity, the researcher must propose a solution using recent findings from the domain knowledge and utilising currently identified solutions (Peppers et al., 2007). This step is an entry point when the process is an objective-centred solution.
- *Design and development:* In this activity, the researcher must establish the functionality and architecture of the artefact, and then develop the actual artefact (Peppers et al., 2007). This stage is an entry point when the process is a design-and development-centred initiation.
- *Demonstration:* This activity illustrates the usage of the artefact for solving a particular research problem. Demonstration includes its usage within experiment, simulation, case study, proof or any other suitable activity (Peppers et al., 2007). The demonstration stage is an entry point when the research is client initiated or context initiated.
- *Evaluation:* This activity requires the researcher to determine the performance of the artefact (March & Smith, 1995). An evaluation activity compares the objectives of the solution against the findings of using the artefact during the demonstration activity (Peppers et al., 2007). In addition, this activity is used to evaluate the usefulness of an artefact and that process aids to validate the artefact.
- *Communication:* This activity is the final process and involves the process of sharing and communicating the problem and the importance of the artefact and its use. This stage communicates the innovations and rigour during design. Furthermore, this stage shares and communicates the effectiveness of the solution when applied to the problem (Peppers et al., 2007).

Figure 1-2 provides a summary and shows how the DSRM process has been applied in this study.

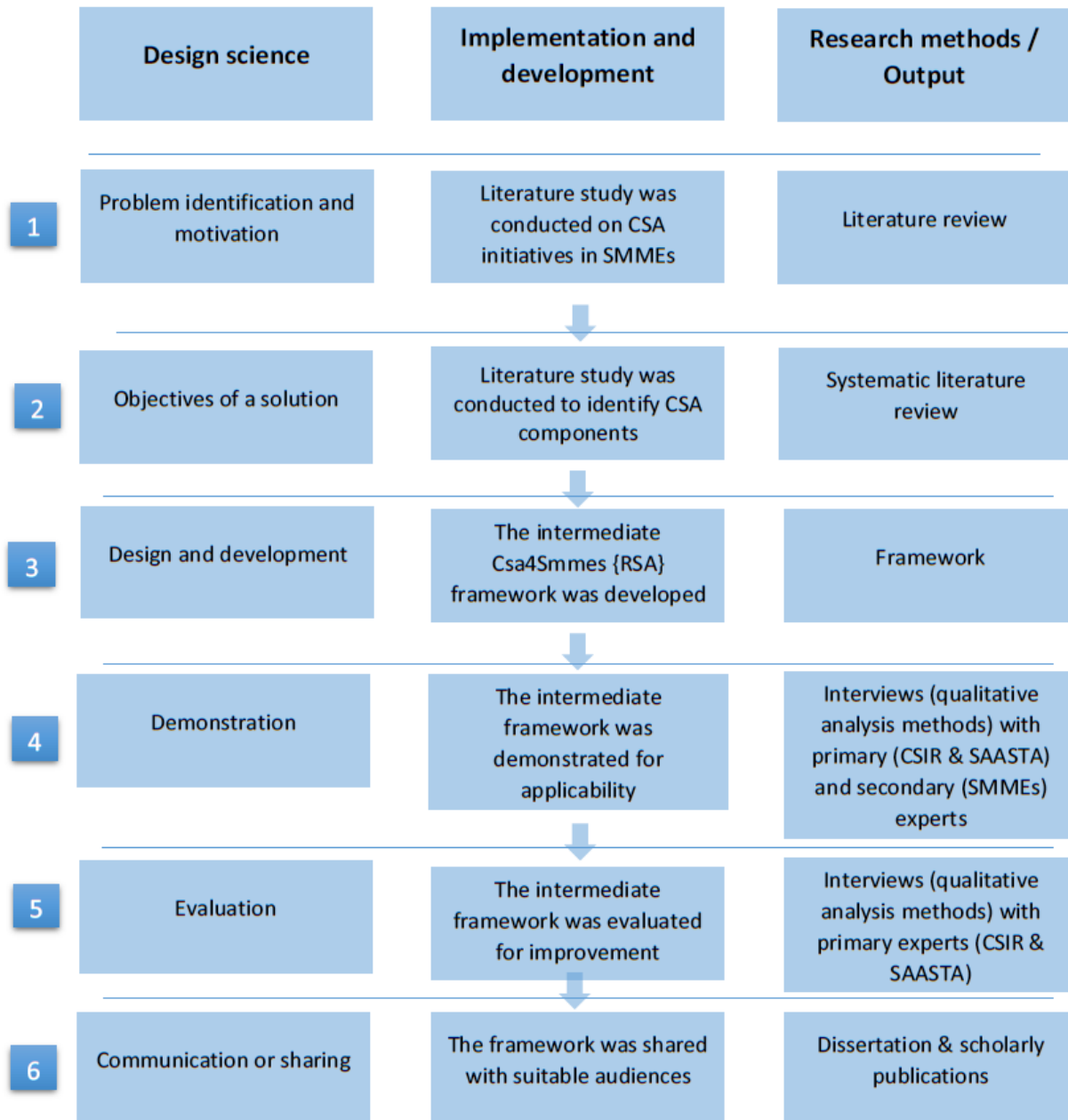


Figure 1-2: Summarised DSRM process applied in the study

The four possible entry points of DSRM are problem-centred initiation, objective-centred solution, design- and development-centred initiation, and client or context initiation. As depicted in Figure 1-1, the first phase concentrates on conducting a literature study to

identify necessary cyber security awareness components that are required to develop the conceptual framework which is referred to as the intermediate Csa4Smme {RSA} framework.

The second phase concentrates on developing the intermediate Csa4Smme {RSA} framework based on identified cyber security awareness components. This phase focuses on selecting relevant cyber security awareness components that are suitable for SMMEs. The intermediate Csa4Smme {RSA} framework will be developed as per the identified components.

The third phase concentrates on demonstrating and evaluating the intermediate Csa4Smme {RSA} framework through expert interviews. This phase is for validating and modifying the intermediate framework to produce a framework for cyber security awareness in South African SMMEs. In addition, the third phase concludes the study by producing a Csa4Smme {RSA} framework that will help the country by securing and protecting SMMEs against cyber attacks that are human-centred.

In conclusion, a detailed methodology will be covered in the next chapter.

## **1.6 ETHICAL CONSIDERATIONS**

The study addresses ethical issues during and after the research has been conducted. Creswell (2013) discusses the importance of addressing ethical issues which are discussed below. Handling ethical issues enables the researcher to protect participants and earn their trust. It inspires the researcher to be honest, and to evade misconduct and offensiveness that might affect participants. Lastly, addressing ethical issues helps to effectively handle new challenging problems as they arise within the study.

The researcher gained permission from participating experts and their respective companies. This identified ethical issue occurred before conducting the study and it was handled by identifying participants and explaining to them what the proposed study entails. After permission has been requested and granted, interviews were conducted to demonstrate and evaluate with the aim of validating the intermediate Csa4Smme {RSA} framework that enhances cyber security awareness for South African SMMEs.

At the beginning of the study, the purpose of the study was discussed with participants. Informal conversations were conducted with experts to discuss the proposed study. Terms and conditions related to the research were disclosed in order to clarify that participants are not forced to participate. The study did not request any harmful personal information from participants. Participants had to decide to either disclose their company name or not. The researcher ensured that participants acknowledge their rights concerning anonymity and privacy. The researcher gave all participants equal amounts of treatment. An informed agreement was required by distributing a message to experts to validate the intermediate Csa4Smmes {RSA} framework. In addition, an ethical agreement letter has been sought from the institutional ethics committee. In conclusion, the results of the study will be shared with participants, SMMEs, experts and other researchers.

## **1.7 OVERVIEW OF CHAPTERS**

The study consists of six chapters whereby Chapter 1 introduces the study by providing background information, the research statement, the research objectives and the general structure of the research project. Subsequently, Chapter 2 will provide a blueprint regarding the methodology that will be implemented to answer the research questions. The research design utilised in this study will be discussed in more detail. Chapter 3 will provide a discussion regarding the importance of cyber security awareness. This chapter will discuss the components of cyber security awareness that will be required to construct the intermediate Csa4Smmes {RSA} framework. Chapter 4 will provide a discussion about the intermediate Csa4Smmes {RSA} framework that will be suitable for SMMEs. The intermediate Csa4Smmes {RSA} framework will be developed. A framework for cyber security awareness in SMMEs (Csa4Smmes {RSA} framework) will be developed in Chapter 5 based on recommendations from expert reviewers. Chapter 5 will discuss findings regarding the demonstration and evaluation of the intermediate Csa4Smmes {RSA} framework. Chapter 6 will provide a summary of the study, conclusions and recommendations regarding the Csa4Smmes {RSA} framework. Chapter 6 will focus on discussing the contribution of the study and a conclusive summary will also be provided.

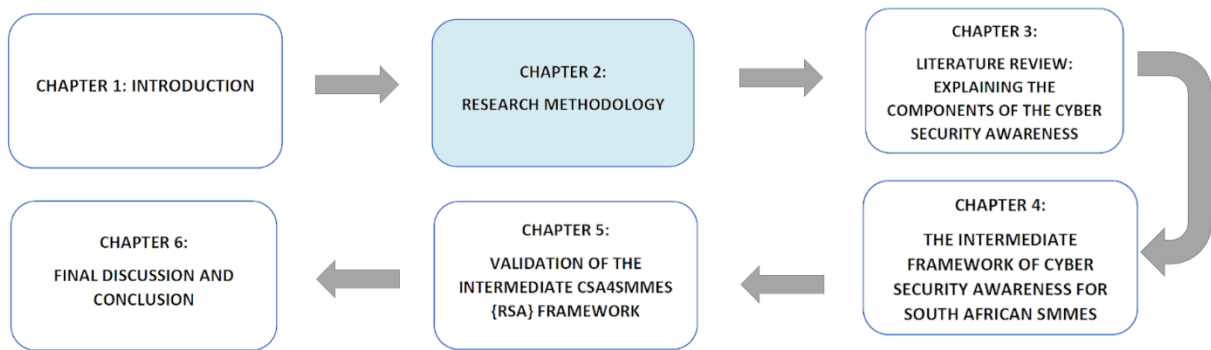


## **1.8 SUMMARY**

This chapter provided background information regarding the research scope to introduce the research study. Furthermore, it provided an overview of the overall structure of the research study, including the problem statement, research questions, literature review, brief research methodology, ethical considerations and overview of chapters.

Chapter 2 provides a detailed discussion regarding the research methodology.

# CHAPTER 2: RESEARCH METHODOLOGY



<b>CHAPTER 2: RESEARCH METHODOLOGY</b>	2.1 INTRODUCTION	2.2 OVERVIEW OF CHAPTER 2
	2.3 RESEARCH DESIGN PROCESS	2.4 DESIGN SCIENCE RESEARCH
	2.5 RESEARCH ETHICS	2.6 SUMMARY

## **2 RESEARCH METHODOLOGY**

### **2.1 INTRODUCTION**

This chapter discusses the DSRM research methodology which was used for this study to answer the research questions.

### **2.2 OVERVIEW OF CHAPTER 2**

Chapter 2 provides more detail regarding the research design process which has been partly discussed in Chapter 1 (section 1.5). Section 2.3 provides a discussion regarding the selected research design process while section 2.4 provides a discussion concerning the research methodology which has been identified for this study. In section 2.5, a discussion concerning research ethics will be provided. Lastly, section 2.6 provides a summary of this chapter.

### **2.3 RESEARCH DESIGN PROCESS**

#### **2.3.1 Research philosophy**

Research paradigms describe the fundamental philosophical understanding of clusters of people about the world in which they reside and the research studies they conduct (Oates, 2006). The research paradigms can be considered as basic sets of beliefs that are responsible to guide action (Creswell, 2014; Guba, 1990). A paradigm in information systems and information technology is for providing guidance in research within this field and in the process of constructing and implementing systems.

A worldview can be described as a common philosophical orientation about the world and the nature of research that a researcher brings to a study (Creswell, 2014). The research philosophy is mainly concerned with rigorously forming, regulating and enhancing the methods which are liable for creating knowledge (Partington, 2002).

The research philosophy displays the perception of a researcher and the starting point for the research, such as the nature of knowledge as observed by the researcher (Bryman, 2016; Buthelezi, 2017). Research philosophies are not in competition with one

another. However, the philosophies vary due to the desired objectives of a study. The selection of research philosophies is based on the suitability and probability of achieving desired objectives (Buthelezi, 2017). The selection of research methods and strategies is dependent on the research philosophical standpoints (Saunders, Lewis, & Thornhill, 2007).

Therefore, based on the philosophical grounding, a discussion regarding the types of research perspectives or paradigms applicable to information systems and information technology and related research (positivist, interpretive, critical research and design science research) follows below.

### 2.3.2 Paradigm

Research paradigms are discussed in terms of characteristics and the suitable paradigms are selected. The possible philosophical assumptions for this study will be adopted from the matrix of Adebisin (2011) as shown in Table 2-1. This table provides a list of important characteristics to be considered in the implementation of the subsequent research paradigms. The research paradigm used for this study is represented by the last column titled “This study” in which N stands for *No*, while Y stands for *Yes*.

**Table 2-1: Philosophical assumptions of the four research paradigms (Adebisin, 2011; Terre-Blanche et al., 2006)**

Research paradigms	Philosophical assumptions				
	Ontology	Epistemology	Methodology	Axiology	This study
Positivist	* Single, stable reality *Law-like	* Objective * Detached observer	* Experimental * Quantitative * Hypothesis testing	* Truth (objective) * Prediction	N
Interpretative	* Multiple realities * Socially constructed	* Empathetic * Observer subjectivity	* Interactional * Interpretation * Qualitative	* Contextual understanding	Y

Research paradigms	Philosophical assumptions				
	Ontology	Epistemology	Methodology	Axiology	This study
Critical/ Constructionist	* Socially constructed reality * Discourse * Power	* Suspicious * Political * Observer constructing * Version	* Deconstruction * Textual analysis * Discourse analysis	* Inquiry is value bound * Contextual understanding	N
Pragmatism	* Practical	* Objective or subjective	* Mixed methods * Quantitative * Quantitative * Design-based research * Action research	* Value-free/ biased	Y

As shown in Table 2-1, only applicable research paradigms will be discussed:

- *Interpretive research paradigm*: In this paradigm, access to reality is shown through social constructs such as language, consciousness, shared meaning and instruments. The focus is on the difficulty of creating human sense (Myers, 2013). An interpretivist believes that reality is disproportionately complicated to regulate every variable in it. The role of the researcher in an interpretative research paradigm is to discover a systematic method of understanding circumstances within its natural setting (Buthelezi, 2017). Based on the interpretivist perspective, researchers attempt to understand in what way participants distinguish between situations (Buthelezi, 2017; Deetz, 1996).
- *Pragmatic research paradigm*: In this paradigm, gaining knowledge is regarded as a continuum (Goles & Hirschheim, 2000). It accommodates studies that do not neatly fit the requirements of positivism or interpretivism (Alghamdi, 2013; Kortjan,

2013). The focus is on choosing methods that are most applicable, appropriate and relevant to the research. In addition, the research is determined by interest, value and relevance (Meyer, 2017; Van Zyl, 2015). If the research is not clearly determined as to whether to adopt an interpretivist or positivist paradigm, then pragmatism is a suitable choice (Buthelezi, 2017; Saunders et al., 2007). March and Smith (1995) and Hevner, March and Park (2004) identify pragmatism as a paradigm relevant to DSRM.

This study used interpretative and pragmatic paradigms to explain the fundamental philosophy depicted in Table 2-1. The pragmatic paradigm is applied to the DSRM and the interpretative paradigm is used in the design, demonstration and evaluation of the artefacts (only during phase 3; see Figure 1-1 and Figure 2-1).

### 2.3.3 Research approaches

The research approach mainly gives details regarding the connection between theory and reality (Bryman & Bell, 2015; Buthelezi, 2017). There are two types of research approaches which can be adopted by a study, namely the deductive and inductive approach as explained in Table 2-2.

**Table 2-2: Deductive and inductive research approach characteristics (Bryman & Bell, 2015; Buthelezi, 2017; Creswell, 2014; Gcaza, 2017; Hesse-Biber & Leavy, 2010; Robson, 2002; Saunders et al., 2007; Silverman, 2013)**

<b>Characteristics of research approaches</b>	
<b>Deductive</b>	<b>Inductive</b>
The research is initiated by developing a research hypothesis.	The research is initiated by observing and searching for patterns in the data.
Examines a theory against data.	Produces a theory from data.

<b>Characteristics of research approaches</b>	
<b>Deductive</b>	<b>Inductive</b>
This approach is suitable for the positivist philosophy.	This approach is more appropriate for interpretive philosophy.
This approach uses scientific principles to confirm data validity and to enable the overview of the research findings.	This approach is recognised as a potential method to decrease possible researcher bias during the process of data collection.
The approach starts from general to particular. In addition, it uses a top-down approach.	The approach starts from particular to general. Therefore, it uses a bottom-up approach.
Quantitative in nature.	Uses a qualitative approach.
Works with variables.	Research content is investigated.

The inductive research approach is the best approach to utilise if there is minimal research that exists towards the research topic (Buthelezi, 2017; Saunders et al., 2007). This approach is much more flexible because it enables the focus of the research to change during the process of the research study, and that provides the researcher with more understanding. In conclusion, the inductive research approach was used in this study based on the discussion provided in Table 2-2. In addition, the inductive approach was used while demonstrating and evaluating the intermediate Csa4Smmes {RSA} framework through expert interviews.

**2.3.4 Research methodology**

A research methodology impacts a series of actions to be undertaken by the researcher throughout the course of collecting data to be used for a study (Myers & Avison, 2002;

Ouma, 2013) in order to answer a set of research questions (Ouma, 2013). A variety of research strategies are derived from qualitative, quantitative and mixed methods research (Creswell, 2014; Ouma, 2013). Qualitative research regularly focuses on words from research participants to develop meanings. In addition, qualitative research pertains to describing small groups. This methodology attempts to find knowledge about a certain occurrence through the interpretation and ability to understand the perceptions of the research participants (Meriam, 1998; Ouma, 2013).

Contrarily, a quantitative methodology focuses on the process of testing research hypotheses to test existing theories (Ouma, 2013; Welman & Kruger, 2001). The mixed methods methodology complements both the qualitative and quantitative methodologies to conduct a particular research study. A combination of the two methodologies is used only during the collection and analysis of data (Creswell, Clack, & Vicki, 2007; Ouma, 2013).

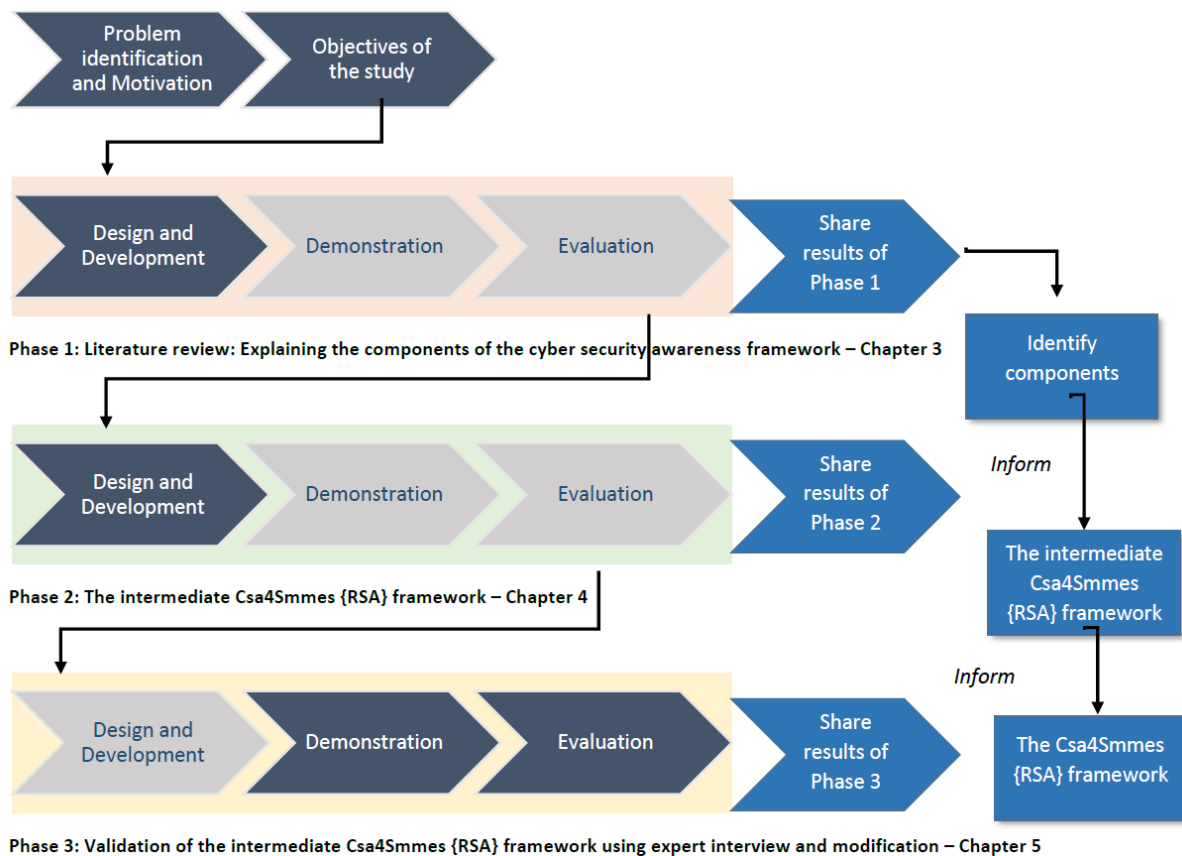


Figure 2-1: Phases of the study: The intermediate Csa4Smms {RSA} framework



Figure 2-1 displays phases of the DSRM process to be followed by the study. The systematic literature review was conducted and analysed qualitatively. In addition, the appropriate methodology for this study is a qualitative methodology because expert interviews were conducted to validate the intermediate Csa4Smms {RSA} framework. The systematic literature review was used to discover research studies that have been conducted on cyber security awareness in South Africa (Phase 1 of Figure 2-1), and to identify components that were required to develop the intermediate Csa4Smms {RSA} framework (Phase 1 of Figure 2-1).

These identified components were used to develop the intermediate Csa4Smms {RSA} framework (Phase 2 of Figure 2-1). Furthermore, expert interviews were conducted to demonstrate and evaluate the intermediate Csa4Smms {RSA} framework to determine its applicability and validity, provide proof of the concept, and to improve and ensure that the Csa4Smms {RSA} framework is suitable for SMMEs (Phase 3 of Figure 2-1). The discussion concerning this DSRM process will be provided in section 2.4.

### **2.3.5 Research strategy**

A research strategy is a process of planning by the researcher and this plan determines how the study will be conducted (Creswell, 2014). The research strategy helps with determining the most suitable method to address the research aims and objectives, and also with monitoring the method of answering the research questions (Buthelezi, 2017; Ezzy, 2013). In addition, research strategies are utilised to answer the research problem and to meet the research objectives.

In information systems research, there are various research strategies that are available for application. Those research strategies include the following: experiments, surveys, case studies, archival studies, ethnography, grounded theory, interviews and systematic literature reviews (Buthelezi, 2017; Hofstee, 2006; Leary, 2016; Swanborn, 2010). However, the selection of the research strategy will be led by the research question(s), research problem and research objectives set by the researcher. Furthermore, the research strategy will be led by the range of existing knowledge, the availability of time

and other resources at hand. In addition, the selection of the strategy will be affected by the philosophical underpinnings (Gcaza, 2017; Saunders et al., 2007).

In conclusion, the DSRM is suitable to answer the research questions related to human problems by establishing artefacts. The output of the study was demonstrated and evaluated through interviewing expert reviewers.

### 2.3.6 Data collection techniques

In research, a variety of instruments can be used to collect the required data to answer certain research questions.

Table 2-3 discusses some of the frequently used research instruments that researchers can use for data collection. The data collection methods used for this study are represented by the last column titled “This study” in which N stands for *No*, while Y stands for *Yes*.

Table 2-3: Data collection techniques (Creswell, 2014; Kumar, 2011)

<b>Data collection types / approach</b>	<b>Advantage</b>	<b>Disadvantage</b>	<b>This study</b>
Questionnaires (Quantitative)	This method is cost-effective and provides greater anonymity.	In this method, responses from participants cannot be supplemented with other information. In addition, this method is a self-selecting bias.	N
Interviews (Qualitative)	Researchers have control over the questions to ask participants.	Researchers might receive biased response from participants.	Y

<b>Data collection types / approach</b>	<b>Advantage</b>	<b>Disadvantage</b>	<b>This study</b>
Systematic literature reviews (Primary and Secondary Documents) (Qualitative)	These allow the researcher to understand the perception of participants better and the information can be accessed at any given time.	Researchers should search hard to find information which is time consuming.	Y
Observation (Qualitative)	Researchers have the ability to record available information.	The researchers can be regarded as intrusions.	N

For this study, a systematic literature review was conducted to discover research gaps and to answer research questions. In addition, the expert interviews were conducted to demonstrate and evaluate intermediate Csa4Smmes {RSA} framework.

### **2.3.6.1 Systematic literature review**

The systematic literature review was conducted and represented by two chapters (Chapter 3 and Chapter 4). This systematic literature study provided an overview concerning South African research studies addressing cyber security awareness. In addition, it provided a discussion about cyber security awareness components as well as existing cyber security awareness models and frameworks that could be used by SMMEs.

The systematic literature review covered the following topics:

- LITERATURE REVIEW: EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK (Chapter 3)

- THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY AWARENESS FOR SOUTH AFRICAN SMMEs (Chapter 4)

Furthermore, the intermediate cyber security awareness framework was developed based on components of the cyber security awareness framework which have been extracted from the systematic literature review.

### **2.3.6.2 Expert review**

The intermediate Csa4Smmes {RSA} framework was demonstrated and evaluated through expert interviews. Purposive sampling was used to select a variety of experts to refine and validate the components of the intermediate Csa4Smmes {RSA} framework as extracted from the literature review.

These experts were selected based on the following experiences:

- Cyber security awareness
- Cyber security practice
- SMME management and operations
- Science and technology awareness

This sampling method allows the researcher to select participants who will provide detailed information (Babbie, 2020; Ouma, 2013; Sami, 2016; Welman & Kruger, 2001). These selected experts were granted access to information about the study, most importantly the intermediate Csa4Smmes {RSA} framework. These expert reviewers were selected based on their experience in the South African research domain and other relevant criteria. The specific number and details of these experts can be found in Table 5-1. In addition, the data collected from interviews were utilised to ensure the validity, reliability and rigor of the study.

In Chapter 5, there is a summary of these expert reviewers who have contributed to the process of demonstrating and evaluating the intermediate Csa4Smmes {RSA} framework.

### 2.3.7 Data analysis

Data analysis is the procedure of interpreting and summarising collected data to discover patterns, relationships and trends within the research area. In qualitative research, data analysis proceeds from data collection to creation of reports based on findings (Creswell, 2014). In addition, to analyse data qualitatively, the researcher must first collect, organise and prepare data. Then the researcher must observe the data collected. Data analysis methods include the following:

- *Thematic analysis*: Thematic analysis is correlated with interviews in terms of analysing the results (Jugder, 2016). This data analysis technique helps with the process of analysing data to provide meaningful information which is understandable.
- *Hermeneutic analysis*: Hermeneutic analysis is related to understanding written information as well as understanding the connection between individuals, organisations and information technology (Myers, 2013). Hermeneutics assists with the process of interpretation because it is concerned with theories related to the proper manner of interpreting text (Schmidt, 2016). In addition, this data analysis technique can be applied when conducting interpretive research.
- *Descriptive statistics*: Descriptive statistics is related to describing, comparing and summarising information numerically (Saunders et al., 2007). Descriptive statistics can be applied by analysing data using tables, charts and graphs.
- *Content analysis*: Content analysis can be defined as a method of conducting a comprehensive and systematic analysis on data in order to identify patterns (Leedy & Ormrod, 2001). This data analysis technique helps with studying and analysing data for similarities or differences to understand the content of data analysed.

In this study, both thematic analysis and hermeneutic data analysis was applied. Thematic analysis was applied for analysing data obtained from expert interviews. Thematic analysis is suitable because it offers a purely qualitative, comprehensive and refinement justification of data (Braun & Clarke, 2006). The systematic literature review was interpreted and analysed using the hermeneutic data analysis because hermeneutic process recommends constant re-interpretation of data to gain a more comprehensive understanding of relevant publications (Boell & Cecez-Kecmanovic, 2010). This process includes reading, analysing, reflective writing and interpretation in a rigorous manner (Lavery, 2003). The hermeneutic data analysis method was also used for interpreting and analysing feedback from expert reviewers. This feedback was used for demonstrating and evaluating the intermediate Csa4Smmes {RSA} framework. In hermeneutic data analysis, it is important for information (in the form of text) acquired from interviews and a systematic literature review to be understood because “the more the process is reiterated (the fusion of horizons achieved), the more comprehensible the text becomes and the ‘greater’ the interpreter's understanding of the text becomes” (Introna, 2011, p. 242). Therefore, the selected data analysis used includes the hermeneutic circle as shown in Figure 2-2.

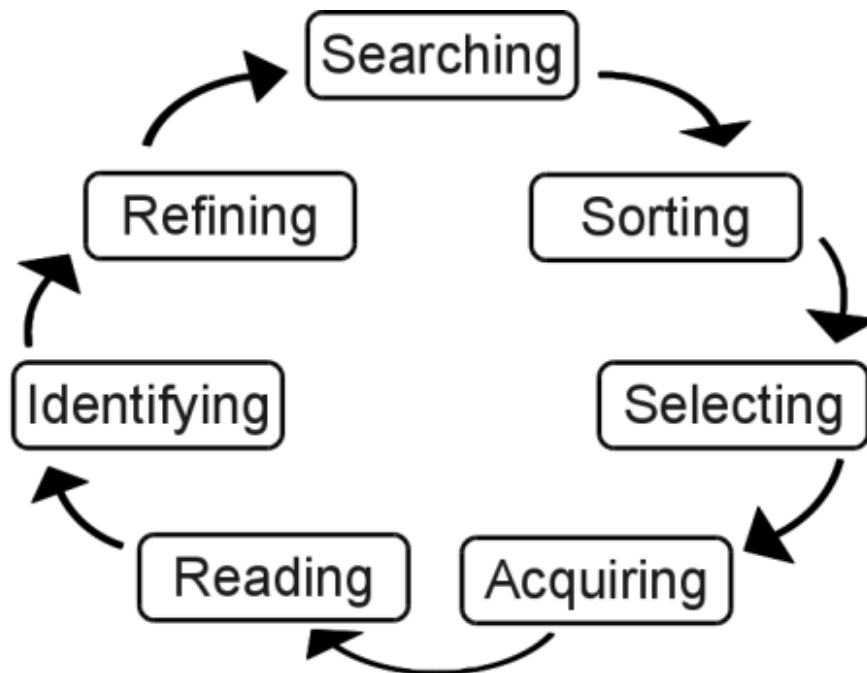


Figure 2-2: The principle of hermeneutic circle, as adapted from Boell and Cecez-Kecmanovic (2010)

Hermeneutic data analysis techniques help to analyse several sectors of written information while considering the complete picture. The principle of hermeneutic circle as shown in Figure 2-2 includes stages to: find relevant information to use, verify if the obtained information is relevant, select important information relating to the study, acquire access to the required information, utilise the information for a certain purpose, select the correct information to be utilised and adjust the information to align with the purpose of the study.

## **2.4 DESIGN SCIENCE RESEARCH METHODOLOGY**

### **2.4.1 Introduction**

The objective of this study is to develop a Csa4Smmes {RSA} framework. Therefore, the DSRM was applied in this study to address the main aim of the research and to provide a response to the formulated research questions.

DSRM is a research approach in which research questions that are relevant to human problems through the establishment of innovative artefacts are answered, thus contributing new knowledge to the body of scientific knowledge. The designed artefacts are both useful and important in understanding the identified problem (Hevner & Chatterjee, 2010). Furthermore, DSRM mainly focuses on creating or advancing an artefact to improve its effectiveness and also validating the artefact by measuring its utility. This section provides a discussion concerning the importance of DSRM and its types of artefacts provided by March and Smith (1995), guidelines of DSRM by Hevner et al. (2004) and the DSRM process of Peffers et al. (2007).

March and Smith (1995) have conducted a study to compare design science (prescriptive research) and natural science (descriptive research). According to March and Smith (1995), DSRM is an activity that uses knowledge with the aim of improving whatever that it is applied to. However, natural science is an activity that produces knowledge with a perception of understanding the domain. Furthermore, March and Smith (1995) highlight that the role of a researcher in DSRM is to produce and apply knowledge of tasks or circumstances to generate effective artefacts. March and Smith (1995) illustrate the

production and application of knowledge through their proposed framework depicted in Figure 2-3.

		<b>Research Activities</b>			
		<b>Build</b>	<b>Evaluate</b>	<b>Theorize</b>	<b>Justify</b>
<b>Research Outputs</b>	<b>Constructs</b>				
	<b>Model</b>				
	<b>Method</b>				
	<b>Instantiation</b>				

Figure 2-3: A research framework (March & Smith, 1995)

In design science, knowledge is applied to build and evaluate the research output (artefact). The next sub-section discusses the research activities of building, evaluating, theorising and justifying (March & Smith, 1995) within the perspective of the six activities of DSRM process (Peffer et al., 2007). Therefore, DSRM can be defined as an approach to build and evaluate IT products with the aim of solving recognised problems within the organisation (Hevner et al., 2004). In DSRM, artefacts are improved until the final version of the artefact meets the requirements of the solution to the problem (Peffer et al., 2007). In DSRM, there are four types of artefacts, namely constructs, models, methods and instantiations (March & Smith, 1995).

In addition, Rossi and Sein (2003) and Puro (2002) added better theories as the fifth output of DSRM (Vaishnavi & Kuechler, 2004). The sixth output is social innovation (Peffer et al., 2007). According to Peffer et al., (2007), social innovation has been added as DSRM output by Van Aken (2004), whereas new properties have been added by Jarvinen (2007).



In DSRM, outputs (artefacts) could be created; however, the discussion below will only cover five artefacts (Hevner & Chatterjee, 2010; Hevner et al., 2004; March & Smith, 1995; Vaishnavi & Kuechler, 2004). These artefacts are the following:

- *Construct*: Is the conceptual vocabulary for describing a problem or solution, and it creates specifications for problems and solutions. A construct must show comprehensiveness, elegance, ease of use and the ability to be understood.
- *Model*: Is a set of statements that can be utilised for expressing the relationships between constructs. Model is a representation of the identified problems and future solutions. Model can also be referred to as a concept and illustration of a problem or solution which includes frameworks and guidelines. In DSRM, models are concentrated on their usefulness or effectiveness. A model must demonstrate dependability to real-life phenomena, accuracy, robustness and reliability.
- *Method*: Is a set of stages that provides guidelines on performing tasks which illustrate a planned series of actions for accomplishing a certain goal. Method can also be defined as a procedure that specifies how to solve identified problems and developing future solutions. In DSRM, a method that intends to effectively solve an existing problem is regarded as valuable. The method must be in operation.
- *Instantiation*: Is the operationalisation of a construct, model or method. Instantiations illustrate the competence, practicability and usefulness of the constructs, models or methods for the environment and its users. The Csa4Smmes {RSA} framework is an example of this artefact.
- *Better theories*: Are the artefact construction as corresponding to experimental natural science. DSRM can contribute by formulating better theories or developing new ones. Developing or evaluating an artefact assists with improving an understanding of the correlation between elements, which could possibly result in the process of developing a new design theory for an artefact.

Therefore, the artefact in this study is an instantiation because this artefact has been established through the development of context from the literature review. This study consists of components that structure a proposed Csa4Smmes {RSA} framework.

## 2.4.2 Design Science Research Methodology process

The DSRM consists of six activities and four potential research entry points as emphasised in Chapter 1 (section 1.6). This sub-section provides a detailed discussion regarding DSRM activities. As shown in Chapter 1, the six activities and four potential entry points of DSRM are illustrated in Figure 2-4 which provides a visual representation of the DSRM process.

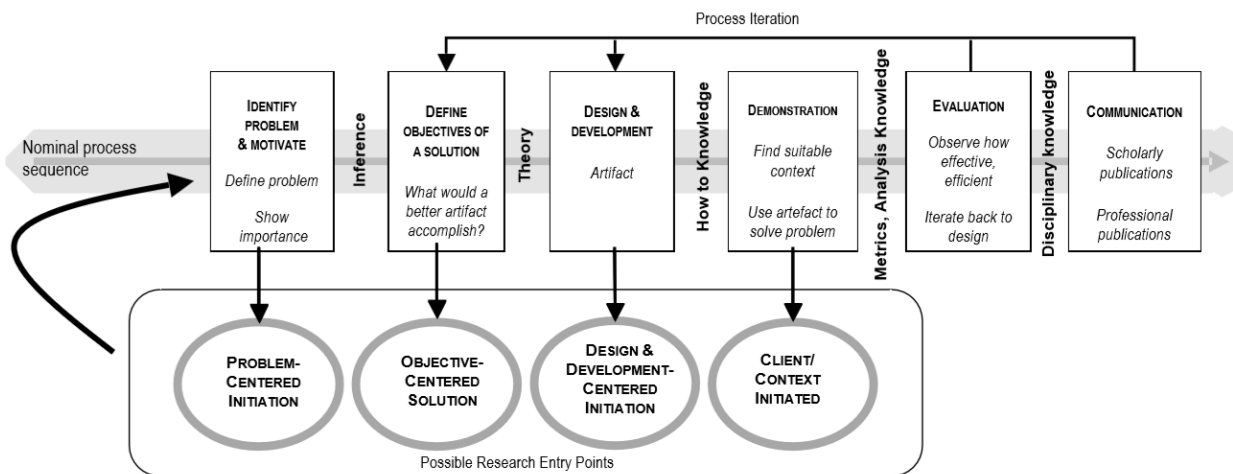


Figure 2-4: DSRM process and possible research entry points (Peppers et al., 2007)

### **Activity 1: Identification and motivation**

The first activity of DSRM is problem identification and motivation. This step requires the researcher to understand the problem and validate the value of a solution. The problem identification process assists with developing an efficient solution in the form of an artefact. Therefore, it might be valuable to approach the problem conceptually in order to capture the complexity of a solution. In addition, it is important to provide motivation for the solution in order to simplify the approval of the findings and clarifies how the

researcher understands the problem (Peppers et al., 2007). This step serves as an entry point when the research is a problem-centred initiation.

*Identification and motivation: Application to this study*

SMMEs in South Africa have inadequate IT skills and financial support required for preventing cyber threats (Von Solms, 2015). In addition, cyber attacks are directed at a variety of organisations regardless of size, financial status or industry. However, SMMEs are impacted the most (Symantec, 2017). Therefore, a systematic literature review was conducted on cyber security awareness and SMMEs. The main objective of this phase is to identify existing cyber security awareness models and frameworks that can be utilised by SMMEs in the context of South Africa. Furthermore, this step entails a literature study to identify current cyber security awareness initiatives in South Africa, mainly to identify those that are designed for SMMEs.

**Activity 2: Defining objectives of a solution**

In this activity, the researcher is required to propose a solution utilising the current body of knowledge and any existing solutions (Peppers et al., 2007). This activity helps to understand the objectives of a solution from the perspectives of problem definition and knowledge to determine possibility and feasibility. In addition, this step is the entry point into the process in an objective-centred solution.

*Defining objectives of a solution: Application to this study*

A systematic literature review was conducted to identify cyber security awareness models and frameworks that can be utilised for SMMEs. Furthermore, it was conducted to identify essential cyber security awareness components which can be utilised to construct the intermediate Csa4Smmes {RSA} framework for SMMEs, particularly those based in South Africa.

**Activity 3: Design and development**

This step focuses on creating artefacts which can be in the form of constructs, models, methods or instantiations. In DSRM, an artefact can be considered any design of an

object where contribution is rooted in the design. In addition, the researcher must establish functionality and architecture of the artefact; then develop the actual artefact. The design and development step is also an entry point when the research is a design and development-centred initiation.

*Design and development: Application to this study*

The intermediate Csa4Smme {RSA} framework was developed and recommended for implementation within SMMEs. Therefore, the intermediate Csa4Smme {RSA} framework should be easily implemented and utilise limited resources that are specifically available for South African SMMEs.

**Activity 4: Demonstration**

This step focuses on the illustration of the building process of the artefact in the problem domain. The demonstration activity and evaluation activity are different because the demonstration activity demonstrates the usage of the artefact in solving a variety of problems. This activity is an entry point when the research is client or context initiated.

*Demonstration: Application to this study*

For this study, the solution was represented in the form of an artefact (intermediate Csa4Smme {RSA} framework). The intermediate Csa4Smme {RSA} framework is provided to help SMMEs in enhancing their internal cyber security awareness for employees, employers and clients. The intermediate Csa4Smme {RSA} framework was demonstrated by interviewing both primary (CSIR and SASTA) and secondary (SMMEs) experts to determine the applicability and to provide proof of the concept. In this study, demonstration and evaluation of the intermediate Csa4Smme {RSA} framework were conducted in parallel through expert reviews because properly implemented evaluation methods could be used to demonstrate the quality of an artefact (Hevner et al., 2004). The selected expert reviewers (primary and secondary) were asked the same set of interview questions for both demonstrating and evaluating the intermediate Csa4Smme {RSA} framework.

### ***Activity 5: Evaluation***

The evaluation step is for determining how well the artefact solves the identified problem (March & Smith, 1995). This step involves comparing the objectives of the solution and the actual results of using the artefact during the demonstration step. At the end of the evaluation step the researcher can choose whether to iterate back to the demonstration step with the aim of improving the effectiveness of the artefact or to proceed to the communication step to allow subsequent projects to improve the artefact further. However, the nature of the research setting can determine whether an iteration is feasible or not.

#### *Evaluation: Application to this study*

The intermediate Csa4Smme {RSA} framework was evaluated for improvement. Furthermore, to evaluate the artefact expert reviewers were selected based on a set of criteria. An interview approach was used, and the data was analysed qualitatively. This intermediate Csa4Smme {RSA} framework was evaluated using a variety of factors as discussed in Chapter 5 to analyse the importance of the proposed cyber security awareness components. The evaluation step was used as an approach to validate the intermediate Csa4Smme {RSA} framework in order to determine the effectiveness and efficiency of its ability to enhance cyber security awareness within South African SMMEs. The intermediate Csa4Smme {RSA} framework was evaluated by the selected primary expert reviewers from the CSIR and SAASTA. This process will be conducted qualitatively. Furthermore, the pragmatic philosophy was supported by the interpretive philosophy only for the demonstration and evaluation phases.

### ***Activity 6: Communication***

The communication activity is the last step of the DSRM process. This step helps to effectively communicate about the identified problem, the importance of the artefact and its usage, the innovations and rigorous nature of the design process and the effectiveness of the solution once applied to the problem (Peppers et al., 2007). Information should be shared with audiences including researchers, technologists (skilled individuals to assist

with initiating and implementing the artefact), management personnel (individuals with the necessary authority for taking decisions to develop or purchase the artefact for implementation) and other people such as practitioners (Hevner et al., 2004; Peffers et al., 2007).

*Communication: Application to this study*

The cyber security awareness framework and resulting findings are consecutively communicated within this dissertation. In addition, the findings will be shared in the form of academic peer-reviewed conference papers and journals.

DSRM is a suitable method for addressing the identified problem in this study because, according to Peffers et al. (2007), design science is mainly associated with producing artefacts for solving real-world problems. DSRM is relevant for this study because of its capability to develop solutions in the form of artefacts that solve human problems (Hevner & Chatterjee, 2010) as well as reinforce the rigour of the process to be followed (Peffers et al., 2007).

Therefore, this study provides a framework that will help SMMEs increase their level of cyber security awareness; additionally to reduce cyber security risks within their organisations and eventually the whole country because compromising cyber security for SMMEs can have a crucial influence on the overall cyber security of the country (Von Solms, 2015). Furthermore, DSRM is likely to make an effective contribution to the body of knowledge within the research area through proper positioning and arrangement (Gregor & Hevner, 2013).

These above-mentioned DSRM process steps shown in Figure 2-1 are aligned with research questions and suitable research methods. This DSRM process illustrates all the phases of the research study. In addition, the next sub-section provides a discussion concerning guidelines to be followed when conducting DSRM.

### **2.4.3 Guidelines for carrying out Design Science Research Methodology**

This sub-section discusses each guideline in detail for carrying out DSRM as provided by Hevner et al. (2004). It also illustrates how each guideline was applied in this study.

#### ***Guideline 1: Design as an artefact***

This guideline refers to the solution in the form of a determined IT artefact which is created to address problems within an organisation (Hevner et al., 2004).

#### ***Guideline 2: Problem relevance***

This guideline worries about the relevance of the research for the information systems community. According to Hevner et al. (2004), the research must address encountered problems and opportunities that are afforded through the collaboration of people, organisations and IT.

#### ***Guideline 3: Design evaluation***

This guideline relates to the gathering and analysis of related data to validate the usefulness, quality and efficiency of the designed artefact (Hevner et al., 2004).

#### ***Guideline 4: Research contribution***

In this guideline, the developed artefact must resolve an unsolved problem or a known problem in a more operational or well-organised manner. Furthermore, the developed artefact must contribute to the existing body of knowledge (Hevner et al., 2004).

#### ***Guideline 5: Research rigour***

This guideline ensures that the research follows the rigorous process to create and evaluate the designed artefact (Niehaves, 2007).

**Guideline 6: Design as a research process**

This guideline emphasises the perception of a well-designed artefact. The search of an effective artefact requires iteration to reach anticipated results (Hevner et al., 2004; Niehaves, 2007).

**Guideline 7: Communication of the research**

In this guideline, Hevner et al. (2004) recommend that findings of the design science research must be well-communicated to a variety of audiences including researchers, technologists, managerial personnel and others.

In conclusion, a table below is provided to indicate how the research study applied the guidelines of DSRM.

**Table 2-4: Guidelines for carrying out design science research methodology**

<b>Guideline</b>	<b>Application to this study</b>
Guideline 1	The study identified the components of cyber security awareness utilised to develop the Csa4Smme {RSA} framework that is tailored and appropriate for SMMEs in the South African context.
Guideline 2	The Csa4Smme {RSA} framework provided a possible solution by contributing to the cyber security culture of South African SMMEs because providing awareness of SMMEs might diminish the risk of successful cyber attacks associated with internet users.
Guideline 3	The Csa4Smme {RSA} framework improved through different phases, starting with the systematic literature review. It has progressed to the identification of relevant cyber security components as well as the development and evaluation of the framework through expert reviews. A cyber security awareness framework integrates all changes as recommended in each phase.



<b>Guideline</b>	<b>Application to this study</b>
Guideline 4	The Csa4Smme {RSA} framework aims to provide valuable insights into the implementation of cyber security awareness within SMMEs in consideration of the South African context.
Guideline 5	To maintain rigour, different approaches such as systematic literature and expert interviews have been utilised to collect data from experts to validate the framework.
Guideline 6	A systematic literature review was used to address several research questions which resulted in identifying relevant components of cyber security awareness.
Guideline 7	The results of the research study was published as a conference paper and dissertation chapters.

**2.5 RESEARCH ETHICS**

A discussion of ethical issues is an unavoidable section to which any researcher should attend. In general, this research process brings tension to the connectivity between the objectives of generalising the research outcomes on behalf of the involved individuals, and the right to preserve the privacy and confidentiality of the participants in the study. They must have a right to anonymity. The participants in a research study must participate voluntarily and sign the consent agreement. This process ensures that participants of the study and any other people are protected from any form of harm during participation. In conclusion, the researcher obtained ethical clearance certificates (APPENDIX B: NO HUMANS INVOLVED (ETHICAL APPROVAL) and APPENDIX C: HUMANS INVOLVED (ETHICAL APPROVAL)) from the University of South Africa (UNISA), issued within the School of Computing. In addition, the researcher obtained approved permission letters from the CSIR and SAASTA (APPENDIX D: PERMISSION LETTERS). Individuals who attended interviews signed the consent form which explains the nature, procedure,

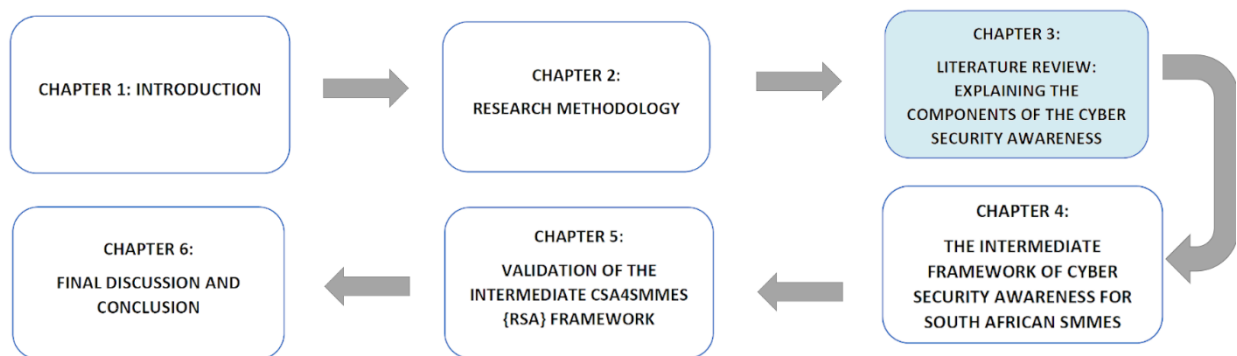
potential benefits and anticipated inconvenience of participation (APPENDIX E: CONSENT FORM). The participant information sheet was also provided to explain the purpose of the research study and how participants will be involved (APPENDIX F: PARTICIPANT INFORMATION SHEET).

## **2.6 SUMMARY**

This chapter discussed the design science research methodology and how it will be applied in this study. In addition, Chapter 2 provided a perspective on the appropriate research paradigm, research design and methodology relevant to the study.

The next chapter discusses the literature review in an attempt to gain insight into existing cyber security awareness studies that have been conducted for South African SMMEs.

# CHAPTER 3: LITERATURE REVIEW: EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK



<b>CHAPTER 3: LITERATURE REVIEW</b>	INTRODUCTION	OVERVIEW OF CHAPTER 3
	3.1	3.2
	SYSTEMATIC LITERATURE REVIEW	CYBER SECURITY AWARENESS
	3.3	3.4
	COMPONENTS FOR CYBER SECURITY AWARENESS FRAMEWORK	SUMMARY
	3.5	3.6

# 3 LITERATURE REVIEW: EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK

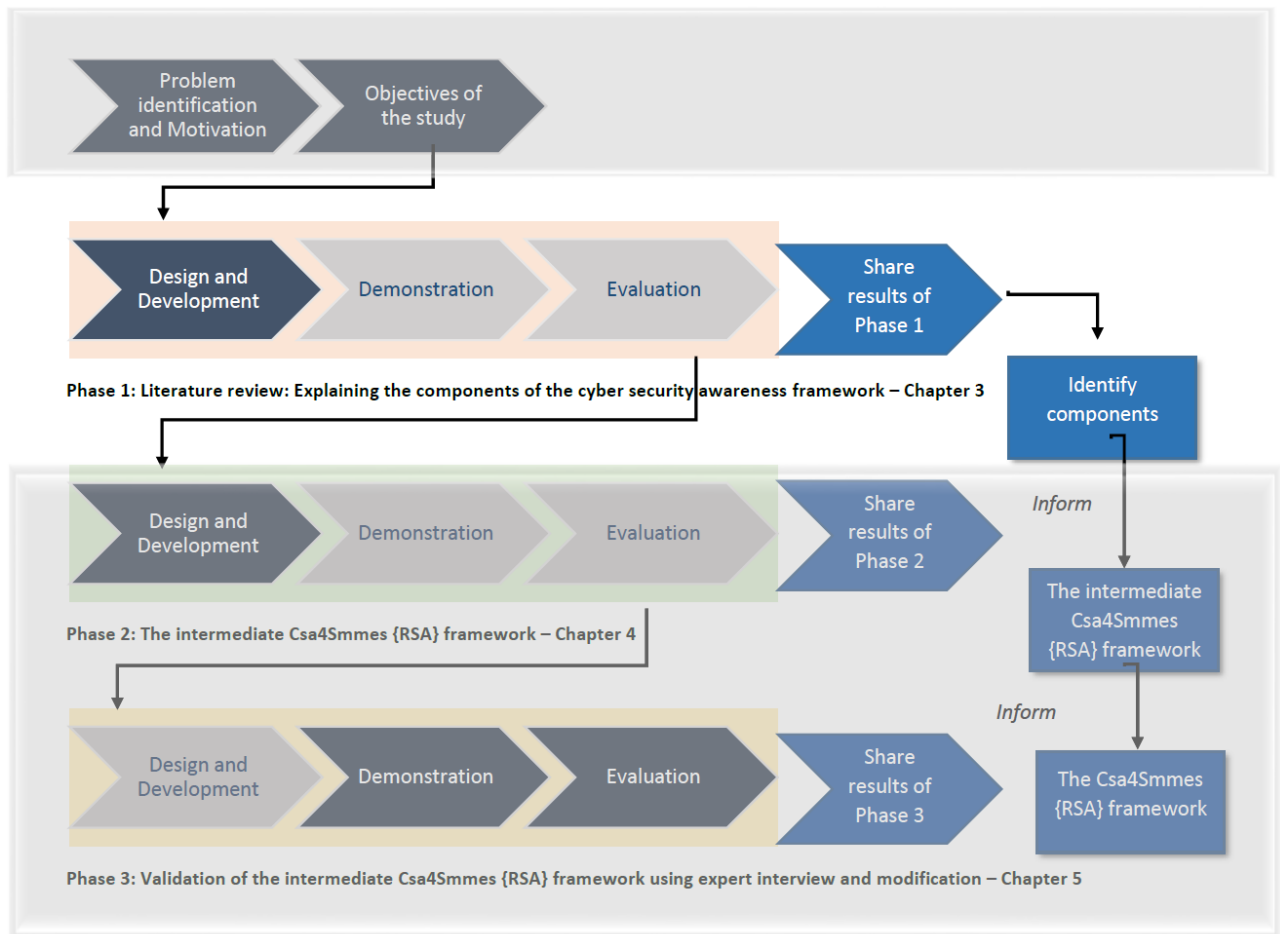
## 3.1 INTRODUCTION

The previous chapter discussed the research methodology which is applied to facilitate the research. The objective of this chapter is to provide an overview of prior cyber security awareness studies conducted in the context of South Africa. Gaps in cyber security awareness in South Africa, which warrant future work, are also identified. A second objective is to find models and frameworks which can be used to identify building blocks for a cyber security awareness framework.

This chapter provides a systematic literature review of cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. The aims of this chapter are to:

- Identify essential components that are required to establish a cyber security awareness framework for SMMEs in South Africa.
- Respond to the following sub-research questions (SRQs):
  - SRQ1: What current studies measure cyber security awareness for SMMEs in South Africa?
  - SRQ2: What existing cyber security awareness models or frameworks can be utilised for SMMEs?
  - SRQ3: What components should be included in a cyber security awareness framework for SMMEs?

Figure 3-1 highlights the DSRM process to be followed by the study.



**Figure 3-1: DSRM Process - Phase 1: Literature study**

As shown in Figure 3-1, this chapter contributes to developing a foundation for the intermediate Csa4Smmes {RSA} framework based on outcomes from Chapter 3. Phase 1 focuses on identifying and explaining cyber security awareness framework components that can be used for developing the intermediate Csa4Smmes {RSA} framework.

The next section provides an overview of the overall structure of Chapter 3.

### **3.2 OVERVIEW OF CHAPTER 3**

This literature review chapter is divided into three segments.

- Segment 1 (Section 3.3) provides a discussion regarding the process followed to conduct the systematic literature review for the study.

- Segment 2 (Section 3.4) provides a discussion about cyber security awareness. In addition, this section provides a discussion concerning existing cyber security awareness models and frameworks.
- Segment 3 (Section 3.5) identifies components that could be included in the cyber security awareness framework.

### **3.3 SYSTEMATIC LITERATURE REVIEW**

This section presents a discussion concerning processes of conducting a systematic literature review. Fink (2010) defines a systematic literature review as an organised, clear, complete and repeatable procedure to identify, evaluate and synthesise the common body of knowledge, and to record existing studies conducted by a variety of academics and practitioners.

A systematic literature review is important to this study because it enables the researcher to identify and summarise existing and relevant cyber security awareness models and frameworks to determine research gaps within the body of knowledge (Agudelo, Jóhannsdóttir, & Davídsdóttir, 2019). Okoli (2015) indorses that if studies aimed to contribute, they should adopt a systematic literature review approach instead of summarising existing literature.

In addition, a systematic literature review on information systems research can be conducted because it is important to document the procedure followed when conducting the review (Okoli, 2015). Petticrew and Roberts (2006) state that a systematic literature review follows a set of scientific methods that clearly aims to limit a systematic error within the study. A systematic literature review commonly attempts to find, assess and synthesise all relevant studies with the aim of answering a particular question or a set of questions.

The systematic literature review originates from the health sciences and it is the most commonly implemented method for generating a persuasive form of scientific body of knowledge for a defined research topic (Lame, 2019). However, in the systematic literature review, there is an activity that requires it to be registered on PROSPERO which is an international open-access database hosted by the University of York

(Centre for Reviews and Dissemination) to avoid duplicated records across all areas of health globally (Borah, Brown, Capers, & Kaiser, 2017).

In addition, the literature must be critically appraised through risk assessment and critical reviewers. These activities have not been considered in this study because the systematic literature review conducted does not apply to the health sciences. Therefore, the eight major steps of conducting systematic literature review presented by Okoli and Schabram (2010) have been adapted and are discussed in the next subsection.

### **3.3.1 Eight major steps in conducting a systematic literature review**

Okoli and Schabram (2010) presented eight steps to be followed when conducting a systematic literature review. These steps are applied as follows (Xiao & Watson, 2019):

1. *Purpose of the literature review:* In the initial stage, the reviewer is for identifying and clarifying the anticipated objectives of the review. The objectives are threefold: (i) to identify research conducted on the subject of cyber security awareness for SMMEs in South Africa, (ii) to identify cyber security awareness models and frameworks that can be utilised by SMMEs and (iii) to identify components for the intermediate Csa4Smme {RSA} framework.
2. *Develop and validate the review protocol:* The review protocol can be defined as a current plan that identifies procedures used for conducting the review and it also helps to improve the rigour of the systematic review. However, this step was excluded in the context of the study because the study was conducted by an individual researcher.
3. *Searching for the literature:* When searching for literature, the reviewer must be clear in unfolding the information. In addition, the reviewer must give details, validate and guarantee the completeness of the search.
4. *Practical screen (screening for inclusion):* In this stage, the reviewer needs to be clear concerning which studies were carried out for review, and which studies were removed without being inspected further.

5. *Quality appraisal (screening for exclusion)*: This stage ensures that the reviewer clearly clarifies the judging criteria on which studies are eligible for review synthesis depending on the quality of the studies.
6. *Data extraction*: Once identifying all articles that must be considered and incorporated in the review, the reviewer must scientifically highlight and acquire only important points in individual studies.
7. *Synthesis of studies*: In this phase, the reviewer should summarise and synthesise information which has been extrapolated from multiple studies through scientific procedures.
8. *Writing the review*: In this phase, the systematic procedure of conducting a literature review must be stated in full details so that the outcomes of the review can be reproduced independently.

### **3.3.2 Academic databases searched**

The academic databases utilised were Google Scholar, IEEE Explore, ACM Digital Library, Scopus, Web of Science, Emerald Insight, Science Direct, SABINET and UNISA WorldCat.

### **3.3.3 Searching the literature**

Document types that have been included are journal articles, books and conference papers. Other types of publications as well as other sections in journals such as “editorials, informal articles from a company/organisation, book reviews, prefaces, article summaries, interviews, news, magazines, trade journals, reviews, correspondence, discussions, comments, letters to the editor, summaries of tutorials, meetings, workshops, panels and poster sessions” have been excluded, (Rahim et al., 2015, p610).

Relevant publications were identified from the period 2000 to 2020 because the review was focused on the recent literature while considering older studies in order to perform a comprehensive search. The main reason for searching for security awareness instead of cyber security awareness was to ensure that the research was rigorous.



During the search, alternative words for SMME (*SME, small company, small business and small organisation*) were used to expand the search results.

### **3.3.4 Inclusion and exclusion criteria**

The inclusion criteria applied for the systematic literature search for cyber security awareness (including models and frameworks) were as follows:

- Studies addressing cyber security awareness or information security awareness.
- Cyber security awareness or information security awareness models and frameworks.
- Only publications written in English.
- Studies addressing cyber security awareness or information security awareness for SMMEs.
- Studies measuring or evaluating cyber security awareness or information security awareness.
- Studies providing a model or framework for cyber security awareness or information security awareness.

The exclusion criteria applied for cyber security awareness (including models and frameworks) were as follows:

- Patent documents.
- Studies referring to cloud computing, security metrics, firewalls, government, politics and legal concepts in the context of cyber security awareness or information security awareness.
- Studies outside the cyber security awareness or information security awareness domain.
- Studies that are focused on information security or cyber security policies.
- Studies that do not propose a cyber security awareness model or framework.
- Cyber security awareness studies that have not been conducted for South Africa.

### 3.3.5 Literature search results

This section provides a discussion regarding the results from the literature research as shown in Table 3-1. The table column headings refer to the following:

- Databases searched to retrieve data.
- Links used to access the databases.
- Total publications retrieved per database searched.

Table 3-1: Databases searched

Database	Link	Total publications
Google Scholar	<a href="https://scholar.google.co.za/">https://scholar.google.co.za/</a>	264
IEEE Explore	<a href="https://ieeexplore.ieee.org/">https://ieeexplore.ieee.org/</a>	196
ACM Digital Library	<a href="https://dl.acm.org/dl.cfm">https://dl.acm.org/dl.cfm</a>	7
Scopus	<a href="https://www.scopus.com">https://www.scopus.com</a>	29
Web of Science	<a href="http://www.webofknowledge.com/">www.webofknowledge.com/</a>	5
Emerald Insight	<a href="https://www.emeraldinsight.com">https://www.emeraldinsight.com</a>	14
Science Direct	<a href="https://www.sciencedirect.com/">https://www.sciencedirect.com/</a>	22
SABINET	<a href="https://journals.co.za/">https://journals.co.za/</a>	4
UNISA WorldCat	<a href="https://unisa.on.worldcat.org/discovery">https://unisa.on.worldcat.org/discovery</a>	3
<b>Total</b>		<b>544</b>

### 3.3.6 Data screening

The information obtained from Table 3-1, was used to provide a visual representation of search results. Figure 3-2 provides information regarding the flow of the literature search and results using the PRISMA method. This PRISMA statement assists

researchers in improving their way of representing systematic reviews and meta-analyses reports (Moher, Liberati, Tetzlaff, Altman, & Group, 2009).

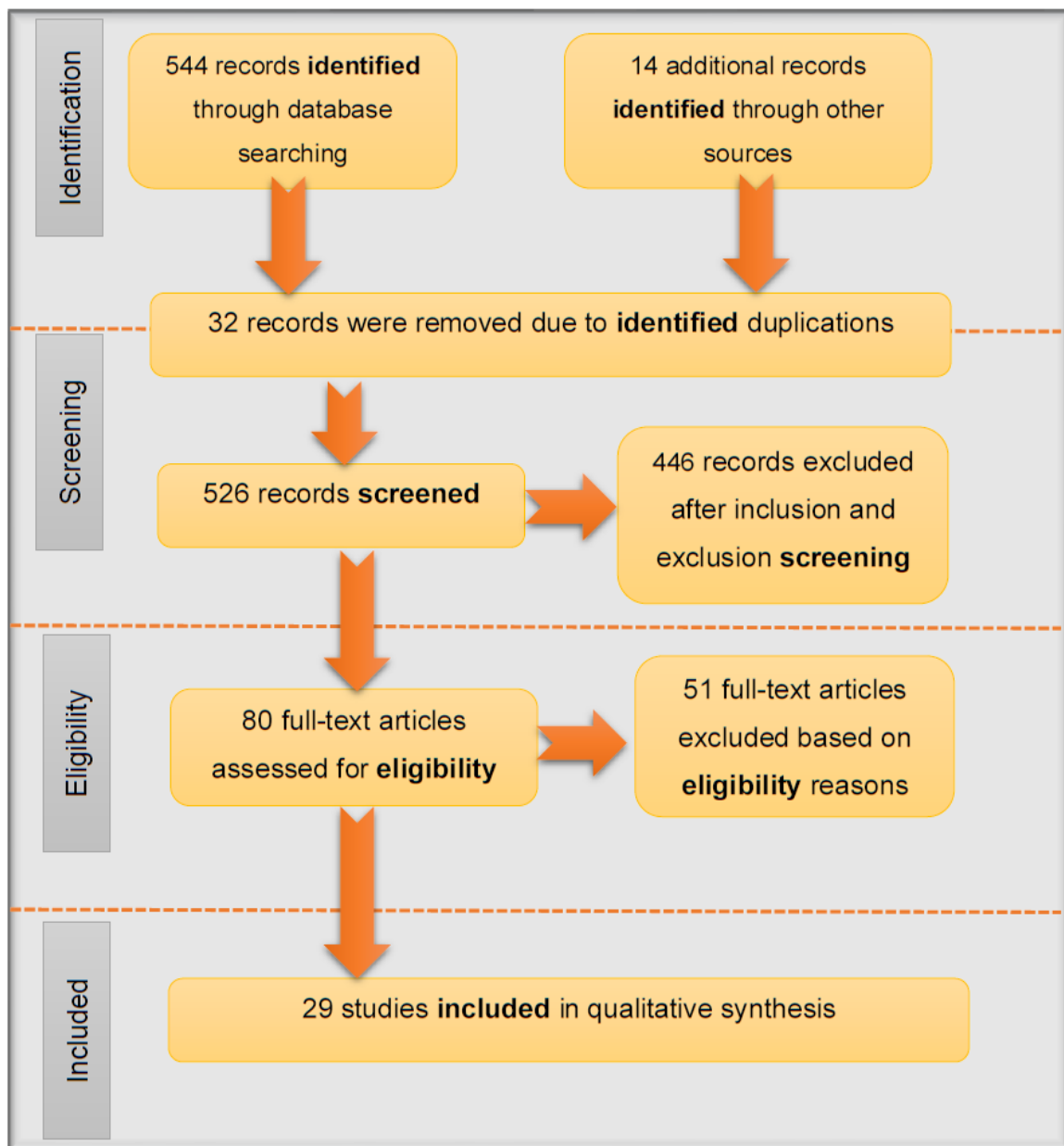


Figure 3-2: Flow chart based on search phases for literature on cyber security awareness for SMMEs

As depicted in Table 3-1 and Figure 3-2, the total number of publications retrieved during the literature search was 558 (544 research articles and an additional 14 theses and dissertations). Figure 3-2 depicts how the inclusion and exclusion criteria were applied. Thirty-two duplicated publications were removed from the search. All unique publications were analysed for inclusion and exclusion by evaluating document titles

and abstracts to obtain information relevant to the research topic. Once titles and abstracts had been evaluated, 446 publications were excluded in the screening step. A total of 80 full-text publications, as shown in Appendix 8-1, were screened for eligibility, reviewed and analysed for relevancy. Appendix 8-1 includes the following column headings which were used in the screening process:

- Publication title.
- Authors.
- Methodology: Identifying whether a quantitative or qualitative method was used.
- Publication type: Identifying whether the publication was a journal or conference publication.
- Research purpose: Providing a summary of the purpose of the research publication.
- Measure: Indicating with an “X” if the research publication focused on measuring the awareness level on cyber security or information security.
- Design and evaluate: Indicating with an “X” if the research publication focused on designing or evaluating cyber security awareness or information security awareness initiatives.
- Models: Indicating with an “X” if the research publication proposed a cyber security awareness or information security awareness model.
- Frameworks: Indicating with an “X” if the research publication proposed a cyber security awareness or information security awareness related framework.
- SMMEs: Indicating with an “X” if the research publication focused on SMMEs in the context of cyber security awareness or information security awareness.
- Included in the study: Indicating with an “X” if the research publication was included in the final set of research papers.

Following the screening process, 51 publications were removed based on the exclusion criteria. A total of 29 full-text publications met the inclusion criteria for this study as indicated in the Figure 3-2.

### 3.3.7 Data analysis and selection

Appendix 8-1 groups and identifies cyber security awareness studies conducted in South Africa. The screening process aids the researcher to identify a list of applicable studies, as indicated in the last column heading, this can be used to answer the research questions. As identified in Appendix 8-1, 51 research studies were not included because they failed to meet the eligibility criteria of the study (shaded rows).

Table 3-2 below gives an overview of the research papers that have been ticked off in the “measure”, “design and evaluate”, “models” and frameworks” categories of Appendix 8-1. This table includes the following column content:

- *Category*: This section groups studies based on the results from Appendix 8-1.
- *References*: This is a collection of studies (references) per category.
- *Research question (RQ)*: The research question that is to be addressed per category.

**Table 3-2: Research categories**

<b>Category</b>	<b>References</b>	<b>RQ</b>
Category 1  Addressing or measuring cyber security awareness or information security awareness level (“Measure” category from Appendix 8-1)	Chandarman & Van Niekerk, 2017; Gundu & Flowerday, 2013b; Jordaan, 2014; Kruger, Drevin, Flowerday, & Steyn, 2011; Kruger, Drevin, & Steyn, 2010; Ngoqo & Flowerday, 2015; Ngoqo & Flowerday, 2014; Shabe, Kritzinger, & Loock, 2017	SRQ1
Category 2  Designing and evaluating current awareness initiatives (“Design and	Amankwa et al., 2016; Amankwa, Loock, & Kritzinger, 2014; Dlamini & Modise, 2012; Grobler, Van Vuuren, & Zaaiman, 2011; Kritzinger, Loock, & Mwim, 2018; Kritzinger, Bada, & Nurse, 2017; Labuschagne, Veerasamy, Leenen, & Mujinga, 2011a;	SRQ3

Category	References	RQ
evaluate” category from Appendix 8-1)	Lejaka, Da Veiga, & Loock, 2019; Von Solms, 2015	
Category 3  Research studies proposing models (“Models” category from Appendix 8-1)	Allam, Flowerday, & Flowerday, 2014; Bada & Nurse, 2019; Gundu & Flowerday, 2013a; Kritzinger & Von Solms, 2010; Kritzinger, 2006; Labuschagne, Burke, Veerasamy, & Eloff, 2011b; Moletsane & Tsibolane, 2020; Potgieter, Marais, & Gerber, 2013	SRQ2 and SRQ3
Category 4  Research studies proposing frameworks (“Frameworks” category from Appendix 8-1)	Dlamini, Taute, & Radebe, 2011; Kortjan & Von Solms, 2014; Kortjan, 2013; Walaza, Loock, & Kritzinger, 2014	SRQ2 and SRQ3

The first category focused on existing studies that addressed or measured cyber security awareness and they were evaluated based on the first sub-research question (SRQ1). This evaluation was conducted to identify studies focusing on cyber security awareness or information security awareness in South Africa. The second category focused on studies that were designing and evaluating cyber security awareness or information security awareness initiatives. These studies were evaluated based on the third sub-research question (SRQ3) which was to identify components required for the intermediate Csa4Smmes {RSA} framework. In this category, only studies that have contributed to the third sub-research question will be adopted. These studies must provide recommendations regarding components of cyber security awareness which can be used to construct the intermediate Csa4Smmes {RSA} framework. The adopted studies were used to support and provide additional content for components identified from adopted models and frameworks. The third and fourth categories focused on studies proposing cyber security awareness or information security awareness models and frameworks. These studies were evaluated based on the

second and third sub-research questions (SRQ2 & SRQ3). In summary, these identified studies were analysed to identify cyber security awareness components required for constructing the intermediate Csa4Smmes {RSA} framework.

The next sub-section provides a discussion on cyber security awareness in South Africa.

### **3.4 CYBER SECURITY AWARENESS**

The objective of this section is to provide a discussion regarding studies conducted to address and measure information security awareness and cyber security awareness in South Africa. These studies were extracted from the first category of Table 3-2. This section answers the first sub-research question (SRQ1). However, a general background is initially provided to discuss the relationship between information security and cyber security, and to provide an overview regarding cyber security awareness.

#### **3.4.1 Relationship between information security and cyber security**

At times information security and cyber security are considered to describe the same phenomenon because they overlap partially (Von Solms & Von Solms, 2018). Furthermore, even though there is a significant intersection between cyber security and information security, these two concepts are not completely equivalent (Von Solms & Van Niekerk, 2013). Information security can be defined as a security process that is designed by organisations to counter the undesirable effect of evading data loss and the unauthorised use of information (Ahlan, Lubis, & Lubis, 2015). Computer security can be defined as controls that are implemented in organisations to provide confidentiality, integrity and availability (CIA) for all-inclusive components of computer systems (Pfleeger & Pfleeger, 2006).

On the other hand, cyber security is a section of information security which is mainly focused on the protection of confidentiality, integrity and availability of digital information assets against internet threats (Von Solms & Von Solms, 2018). Cyber security goes beyond the limitations of traditional information security. It does not only focus on protecting information resources, but it also protects other assets, including people (Von Solms & Van Niekerk, 2013).

Lastly, cyber security is a collection of technologies, procedures and developments put in place to protect networks, computers, programs and data from outbreak, damage or unauthorised access (Kent et al., 2016). Cyber security is the protection of cyberspace, digital data, ICT technologies and users of cyberspace (Von Solms & Van Niekerk, 2013). Therefore, this study focuses on cyber security which goes beyond the boundaries of information security and ICT security as depicted in Figure 3-3. This figure shows the relationship between information security and cyber security.

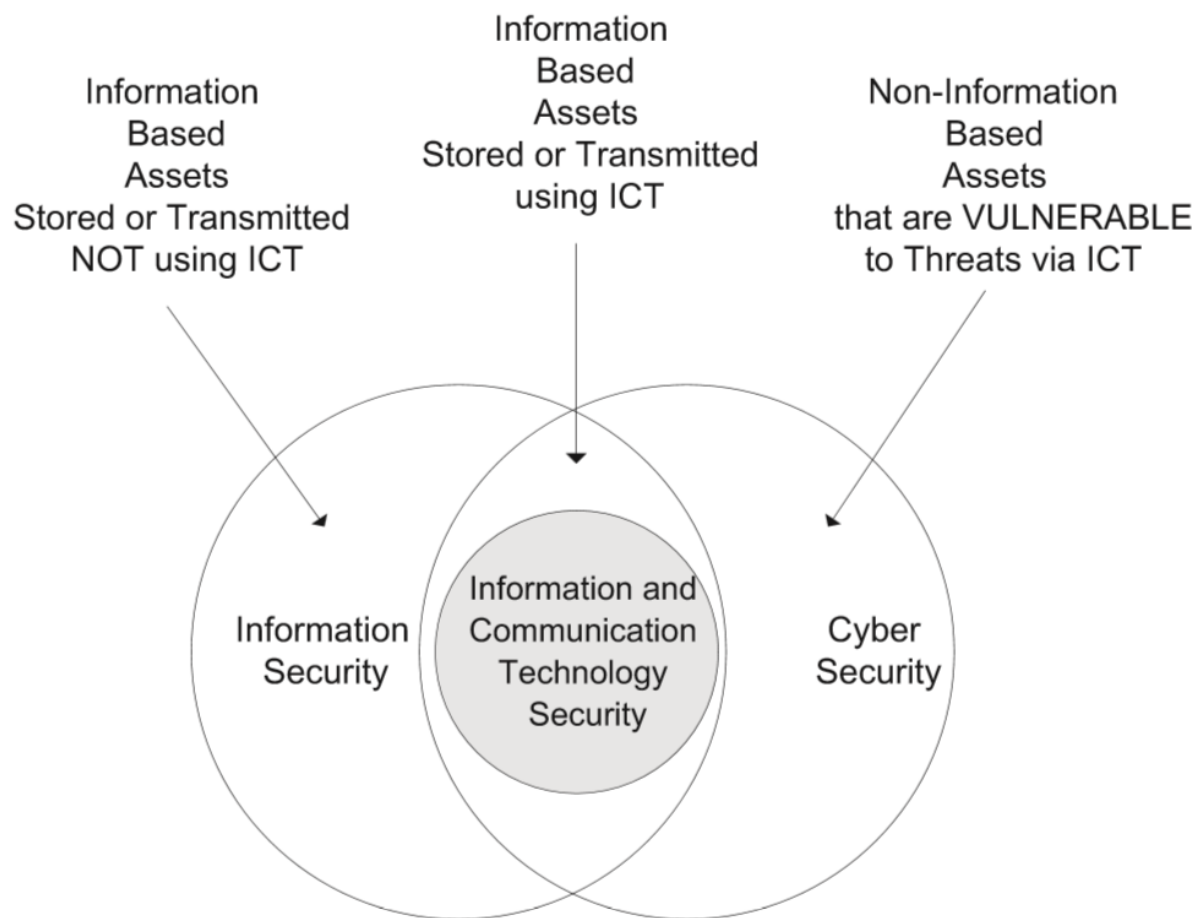


Figure 3-3: Relationship between information security, ICT security and cyber security (Von Solms & Van Niekerk, 2013)

This figure focuses on non-information-based assets that are vulnerable to threats via ICT. Von Solms and Van Niekerk (2013) use Figure 3-3 to emphasise that, regardless of using *cyber security* as an equivalent term for *information security*, cyber security varies from information security. As shown in Figure 3-3, information security has extended from the concepts of ICT security with the aim of protecting the information,



regardless of its recent form and setting, while cyber security is perceived as an extension of information security. Therefore, cyber security focuses on protecting information and information systems resources of an individual or an organisation.

In addition, Von Solms and Van Niekerk (2013) state that cyber security focuses on the protection of individuals utilising the resources within a cyber environment and other related assets. Information security relates to the protection of information (asset) against possible harm caused by threats and vulnerabilities. However, cyber security does not only focus on the protection of cyberspace itself, but also focuses on the functionalities conducted within cyberspace and any other related assets accessible via cyberspace.

### **3.4.2 Overview of cyber security awareness**

Based on the discussion above, this study focuses on cyber security awareness because it can be defined as the protection of confidentiality, integrity and availability of information in cyberspace (Von Solms & Von Solms, 2018). Its main aim is to protect information in order to ensure that the availability, confidentiality and integrity of information are not compromised in any way (Kritzinger & Smith, 2008). Cyber security awareness aims to improve the understanding of users towards the implications of their actions from a security perspective (Tariq, Brynielsson, & Artman, 2014).

When conducting cyber security awareness, it is essential to assist all internet users (including employees, employers, clients, suppliers, and customers) within the organisation to have the same basic understanding towards cyber security awareness, policies, and procedures (Dominguez, Ramaswamy, Martinez, & Cleal, 2010). Kruger, Drevin and Steyn (2006) state that cyber security awareness should ensure that all users of the internet are equipped enough to comply with the cyber security policy in their workplaces. Cyber security awareness should help all internet users within organisations to be aware of cyber security threats directed at their organisations.

Cyber security awareness is a state where internet users are aware of and dedicated to cyber security procedures, understand the significance of individual duties regarding cyber security and act accordingly (Pattinson et al., 2017). Cyber security awareness helps top management and security professionals with an opportunity to successfully communicate with employees regarding the importance of cyber security, the

organisational security policy and other important cyber security related information (Abawajy, Thatcher, & Kim, 2008). Cyber security awareness focuses on changing the culture and behaviour of internet users within the organisation in terms of cyber security (Hassanzadeh, Jahangiri, & Brewster, 2013) and also concerning what needs to be protected from whom and how (Al Awawdeh & Tubaishat, 2014). This enables individuals within an organisation to conduct secured activities. Cyber security awareness educates users by emphasising the importance of protecting information and its associated threats that may affect that particular type of information.

Cyber security awareness assists internet users in understanding the importance and implications of cyber security policies, rules and guidelines. In addition, it provides organisations with an ability to understand the behaviour of employees regarding policies, rules and guidelines (McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017). It is essential to conduct cyber security awareness for individuals within the organisation to determine their security-related behaviour in both organisational and private contexts. Individuals with limited or no cyber security awareness cause the organisation to be prone to cyber criminals. Furthermore, the protection of information is not only a business requirement, but also a legal and ethical requirement (Al Awawdeh & Tubaishat, 2014).

Cyber security awareness can be used as an effective method of addressing cyber security because this initiative helps to minimise costs of security incidents (Al Awawdeh & Tubaishat, 2014). In addition, awareness is an effective method that costs less and reduces the overall security expenses compared to training and education. In general, awareness helps users to be responsible for protecting the confidentiality, availability and integrity of the organisational information.

The main goal of cyber security awareness is to reduce cyber security faults caused by humans. It also increases employees' understanding relating to their responsibilities and penalties linked with such faults (Al Awawdeh & Tubaishat, 2014). Therefore, it is important to provide up-to-date cyber security awareness to keep cyber security existing in the minds of internet users within organisations. Although, in order to obtain effective awareness results, cyber security awareness should distinguish between clusters of users in order to deliver relevant and customised information to that specific audience (Al Awawdeh & Tubaishat, 2014).

Cyber security awareness in this study is seen as an essential approach to increase the levels of knowledge and awareness to help naive users in recognising and preventing cyber attacks associated with human interactions. Cyber security awareness is an effective method to secure cyberspace.

This section has clarified the difference between information security and cyber security. Therefore, the next sub-section answers the first research question (SRQ1).

### **3.4.3 Cyber security awareness in South Africa**

This sub-section provides a discussion regarding studies that are conducted on cyber security awareness for SMMEs in South Africa. The following is a discussion on the studies identified in the systematic literature review to address the first research question (SRQ1), namely:

*What current studies measure cyber security awareness for SMMEs in South Africa?*

Several scholars conducted cyber security awareness for different objectives and a variety of target audiences. Based on data from the systematic literature review, a list of studies was identified as depicted in Table 3-3. This table presents a list of studies that met inclusion criteria as identified in Figure 3-2 and Table 3-2. The studies included in Table 3-3 were derived from the first category of Table 3-2, namely “measure”. This category identifies South African studies that measure the level of cyber security awareness and information security awareness. These table column headings carry the following meanings:

- Authors: Contributors towards the research study.
- CSA: Cyber security awareness related research studies.
- ISA: Information security awareness related research studies.
- SMMEs: Studies conducted for SMMEs.
- Students: Studies conducted for students.
- Mobile phone users: Studies conducted for mobile device users.
- Ordinal users: Studies conducted for ordinary users.

- Level of awareness: Studies conducted to measure the level of security awareness.
- Knowledge, attitude and behaviour: Studies that measure awareness based on knowledge, attitude and behaviour.

An “X” indicates if the research publication in column 1 has focused on the column heading.

**Table 3-3: Matrix analysis (awareness scope) of studies measuring cyber or information security awareness levels (from Category 1 of Table 3-2)**

<b>Authors</b>	<b>CSA</b>	<b>ISA</b>	<b>SMMEs</b>	<b>Students</b>	<b>Mobile phone users</b>	<b>Ordinal users</b>	<b>Level of awareness</b>	<b>Knowledge, attitude and behaviour</b>
1. Chandarman & Van Niekerk (2017)	x			x			x	x
2. Shabe et al. (2017)	x				x		x	
3. Ngoqo & Flowerday (2015)		x		x	x		x	x
4. Ngoqo & Flowerday (2014)		x		x	x			x
5. Jordaan (2014)		x	x				x	x
6. Gundu & Flowerday (2013b)		x	x					x
7. Kruger et al. (2011)		x		x			x	x
8. Kruger et al. (2010)		x		x			x	x

The studies included in Table 3-3 were used to identify the research focus. This table portrays a shortage of academic studies on cyber security awareness for SMMEs as discussed in the next sub-section.

#### **3.4.4 Discussion of studies in Table 3-3**

Both cyber security awareness and information security awareness studies were included for analysis to identify the general trend regarding security awareness in South Africa. This trend is mainly to measure information security awareness levels while considering knowledge, attitude and behaviour of the target audience (Gundu & Flowerday, 2013b; Jordaan, 2014; Kruger et al., 2010; Kruger et al., 2011; Ngoqo & Flowerday, 2014; Ngoqo & Flowerday, 2015).

Research studies focussing on cyber security awareness and information security awareness are presented mostly to school learners and university students (Chandarman & Van Niekerk, 2017; Kruger et al., 2010; Kruger et al., 2011; Ngoqo & Flowerday, 2014; Ngoqo & Flowerday, 2015) and there is less focus on cyber security awareness for SMMEs.

As identified in Table 3-3, a research gap has been identified whereby a cyber security awareness study has not been conducted for South African SMMEs in terms of measuring the cyber security awareness level. However, a study was conducted to identify information security awareness levels for SMMEs that depend on IT for successful business operations (Jordaan, 2014). In general, there seems to be more South African studies focusing on information security awareness (Gundu & Flowerday, 2013b; Jordaan, 2014; Kruger et al., 2010; Kruger et al., 2011; Ngoqo & Flowerday, 2014; Ngoqo & Flowerday, 2015) than on cyber security awareness (Chandarman & Van Niekerk, 2017; Shabe et al., 2017).

In conclusion, the first sub-research question (SRQ1) was answered. The next sub-section attempts to respond to the second sub-research question (SRQ2).

#### **3.4.5 Cyber security awareness models and frameworks**

This sub-section discusses existing cyber security awareness models and frameworks as identified in Table 3-2 and relating to the second sub-research question (SRQ2), namely:

*What existing cyber security awareness models and frameworks can be utilised for SMMEs?*

Table 3-4 provides a list of existing models and frameworks as extracted from Table 3-2 for the third and fourth categories. These existing models and frameworks can be utilised or adopted to enhance the level of cyber security awareness within the community of SMMEs in South Africa. The column headings refer to the authors, publication titles and aims of their studies.

**Table 3-4: Existing cyber security awareness models and frameworks (from Categories 3 and 4 of Table 3-2)**

<b>Authors</b>	<b>Title</b>	<b>Aim</b>
1. Bada & Nurse (2019)	“Developing cyber security education and awareness programmes for small and medium-sized enterprises (SMEs)”	Proposes a high-level cyber security education and awareness programme to be applied in SMMEs located in cities.
2. Walaza et al. (2014)	“A framework to integrate ICT security awareness into the South African schooling system”	Assesses previous and present models and frameworks with the aim of formulating and proposing a framework tailored for the South African education system and environment.
3. Kortjan (2013); Kortjan & Von Solms (2014)	“A conceptual framework for cyber security awareness and education in SA”	Proposes a cyber security awareness and education framework for South African internet users.
4. Allam et al. (2014)	“Smartphone information security awareness: A victim of operational pressures”	Presents a model that can be applied in designing policy, procedure and controls to enable the ISA level to be included as a continuous assessment.

<b>Authors</b>	<b>Title</b>	<b>Aim</b>
5. Gundu & Flowerday (2013a)	"Ignorance to awareness: Towards an information security awareness process"	Provides an ISA process to promote positive security behaviour using a behavioural intention.
6. Labuschagne et al. (2011b)	"Design of cyber security awareness game utilizing a social media framework"	Proposes an interactive game to create awareness of information security threats and vulnerabilities.
7. Dlamini et al. (2011)	"Framework for an African policy towards creating cyber security awareness"	Proposes a high-level African cyber security policy and an African CSA framework to guide cyber security agencies, standards, legislation and other initiatives to promote cyber security awareness.
8. Kritzinger & Von Solms (2010)	"Cyber security for home users: A new way of protection through awareness enforcement"	Proposes a process that can be used to provide and enforce ISA to home users.
9. Potgieter et al. (2013)	"Fostering content-relevant information security awareness through browser extensions"	Presents a browser extension that promotes security values and provides security suggestions based on users' behavioural patterns.
10. Kritzinger (2006)	"An information security retrieval and awareness model for industry"	Provides a model to address and enhance ISA in industry.
11. Moletsane & Tsibolane (2020)	"Mobile information security awareness among students in higher education: An exploratory study"	Proposes mobile information security awareness.

The studies from Table 3-4 will be discussed because the aim of this sub-section is to answer the identified research questions. Furthermore, as depicted in Table 3-5, the researcher defined factors to analyse each identified model or framework based on the level of operation, target audience, evaluation status, and if adopted in the study.

- *Focus level:* The level where the model or framework was applied (at national level, organisational level or at a particular societal level).
- *Target audience:* The identified target within the model or framework (SMMEs, learners and internet users).
- *Evaluation method:* This table heading determines if the model or framework has been evaluated by the researcher through observational, interviews, testing, simulation, case study, questionnaire, experimental, or any other relevant method (Geerts, 2011).
- *Adopted:* Indicating if the model or framework has been adopted for identifying components for constructing the intermediate Csa4Smme {RSA} framework. These adopted studies contribute to constructing the intermediate Csa4Smme {RSA} framework.

The column headings are indicated with an “X” if the model or framework has focused on that particular table heading. These security awareness models and frameworks included in Table 3-5 have been extrapolated from the systematic literature review.

**Table 3-5: Matrix analysis of cyber security awareness models and frameworks identified**

Security awareness models and frameworks	Focus level			Evaluation	Target audience			Adopted
	National level	Organisational level	Societal level		SMMEs	School learners	Internet users	
1. “Developing cyber security education and awareness programmes for small- and		x			x			x



Security awareness models and frameworks	Focus level			Evaluation	Target audience			Adopted
	National level	Organisational level	Societal level		SMMES	School learners	Internet users	
medium-sized enterprises (SMEs)" (Bada & Nurse, 2019)								
2. "A framework to integrate ICT security awareness into the South African schooling system" (Walaza et al., 2014)	x					x		x
3. "Smartphone information security awareness: A victim of operational pressures" (Allam, Flowerday, & Flowerday, 2014)		x		x			x	
4. "Ignorance to awareness: Towards an information security awareness process" (Gundu & Flowerday, 2013a)		x		x	x			x
5. "A conceptual framework for cyber security awareness and education in SA" (Kortjan, 2013; Kortjan & Von Solms, 2014)	x			x			x	x
6. "Design of cyber security awareness game utilizing a social media framework" (Labuschagne et al., 2011b)			x				x	
7. "Framework for an African policy towards creating cyber security awareness" (Dlamini et al., 2011)	x						x	x
8. "Cyber security for home users : A new way of protection through awareness enforcement" (Kritzinger & Von Solms, 2010)			x				x	
9. "Fostering content-relevant information security awareness through browser extensions" (Potgieter et al., 2013)		x		x			x	

Security awareness models and frameworks	Focus level			Evaluation	Target audience			Adopted
	National level	Organisational level	Societal level		SMMES	School learners	Internet users	
10. "An information security retrieval and awareness model for industry" (Kritzinger, 2006)		x		x			x	x
11. "Mobile information security awareness among students in higher education: An exploratory study" (Moletsane & Tsibolane, 2020)		x		x		x		

As depicted in Table 3-5, it was discovered that models and frameworks mostly focused on organisational and national levels respectively. In addition, most models and frameworks were proposed to enhance security awareness for internet users more than other target audiences.

Evaluation is considered a crucial component of the research process (Kortjan, 2013; Kortjan & Von Solms, 2014) and therefore these models and frameworks must be evaluated as well. As identified in Table 3-5, six out of eleven models and frameworks have not been evaluated.

In this section, existing security awareness models and frameworks were identified to answer the research question. The motivation for adopting certain models and frameworks was based on the discussion in the next sub-section which provides a discussion in alignment with column headers of Table 3-5 about the identified models and frameworks.

### 3.4.6 Discussion of studies in Table 3-5

The first study proposed a high-level cyber security awareness and education awareness programme that could be applied in SMMES (Bada & Nurse, 2019). This study used information from a case study and existing studies to build the programme.

The existing studies were analysed to obtain components for building the programme. In addition, the study also provided recommendations. This programme operated at the organisational level, specifically SMMEs. The programme was customised for city-level SMMEs based in developed countries.

This programme was considered when constructing the intermediate Csa4Smme {RSA} framework. However, it may not work effectively because this programme has been designed for SMMEs in cities of developed countries. In general, SMMEs in developing countries are constrained by internal organisational factors of budget, management support and attitudes. Therefore, the proposed programme was adopted by this study but it may not fit perfectly for South African SMMEs. In addition, this proposed programme has not been evaluated.

The second study identified existing information communication technology (ICT) security awareness models and frameworks (Walaza et al., 2014). The study formulated and proposed an ICT security awareness framework tailored for the South African education system and environment, and this study operated at national level. In this study, an in-depth literature review was conducted to identify existing frameworks. A gap analysis of previous and present frameworks was conducted with the aim of formulating and proposing a tailored framework. Each framework was analysed to identify building blocks for the proposed framework.

The framework was adopted in this study; however, it is not recommended for SMMEs because it does not focus on cyber security awareness and has not been evaluated. In addition, the framework is formulated to integrate ICT security awareness into the schooling system.

The third study done by Allam et al. (2014) proposed a model to ensure that organisations were prepared effectively to have control over their information security awareness status. This model helped with monitoring the boundaries and day-to-day issues that affected the organisations. Furthermore, this model allowed organisations to design effectively integrated policies and procedures to encourage good security practice (Allam et al., 2014). The model operated at the organisational level and it was evaluated through an expert review process. Four experts were selected from academia and three with industrial backgrounds. However, this model was not

adopted because its structure does not contribute to establishing the intermediate Csa4Smmes {RSA} framework. The model does not focus on cyber security awareness, and it is not designed for SMMES.

The fourth study conducted by Gundu and Flowerday (2013a) provided a process that SMMEs could follow to ensure that individuals within a particular SMME were aware of information security. The process was constructed based on a behavioural intention model and represented in the form of flowcharts (Gundu & Flowerday, 2013a). This process emphasised that, while planning a security awareness programme, it was important to initially evaluate the existence of a latest information or cyber security policy which had to reflect an organisation's complete status of information security. In addition, based on the initial step, the organisation might have to draft or update an information or cyber security policy.

After having carried out these steps, an organisation could measure current security awareness levels for individuals to identify gaps in their understanding of security awareness. Then a need assessment was carried out to identify an organisation's training and awareness requirements. Based on this process, the organisation had to check if the current awareness levels of information or cyber security were satisfactory. If the awareness levels were not acceptable, awareness and training initiatives had to be conducted to improve them. However, the process iterated until the awareness levels were satisfactory. The model was designed to operate at organisational level. This model was evaluated in a South African engineering SMME and provided good insight regarding the process of conducting successful security awareness; therefore, it was adopted in the current study.

The fifth study by Kortjan (2013) proposed a cyber security awareness and education framework for assisting in creating a cyber-secure culture in South Africa among all internet users. This framework operated at national level and was evaluated through elite interviews. Experts (a cyber security specialist and researcher as well as a research group leader of the Cyber Defence for Scientific Research division at the Council for Scientific and Industrial Research, also known as CSIR) were interviewed to evaluate the proposed framework.

This framework was adopted for SMMEs because they have been identified as one of the target audiences. However, this framework is partially suitable for SMMEs because it is based on a comparative analysis of national cyber security strategies and initiatives towards cyber security awareness and education in countries such as the US, UK, Australia, and Canada. The framework, therefore, may not fit perfectly because it has not been designed specifically for SMMEs but for general internet users in the respective countries.

The sixth study by Labuschagne et al. (2011b) developed an interactive web-based game that helped in enhancing the awareness levels for information security threats and vulnerabilities. This game was hosted through social networking sites for easy accessibility. This study aimed to illustrate the usefulness of using virtual tools to raise cyber security awareness. The interactive web-based game evaluated and educated users in potential security threats and vulnerabilities. In addition, the game operated at the societal level and it was not evaluated. This study does not contribute to identifying the required components for constructing the intermediate Csa4Smme {RSA} framework and was not adopted in the current study.

The seventh study carried out by Dlamini et al. (2011) proposed a high-level African cyber security policy and an African CSA framework to guide cyber security agencies, standards and legislation as well as specific initiatives to promote cyber security awareness. This study proposed a flexible framework that could be adopted in any country's cyber security policy to initiate and maintain awareness programmes. This framework was adopted for SMMEs because it was constructed "through the analysis of a few cyber security policies from developed countries (USA, UK, Estonia and Korea)" (Dlamini et al., 2011, p15) and by African countries with similar existing policies and other cyber security role players, including "agencies, workgroups, forums, conferences, organisations and other initiatives" (Dlamini et al., 2011, p15). In addition, this framework used the National Cyber Security Policy Framework (NCPF), national policies, legislative procedures and laws as its core foundations. This framework might not work effectively for SMMEs because it was anticipated for internet users and not specifically for SMMEs. Furthermore, this framework was designed to operate at national level and not validated.

The eighth study by Kritzinger and Von Solms (2010) proposed a model to enhance cyber security awareness for home users. This model enforced home users to absorb information security content. The model provided home users with up-to-date content regarding information security risks that they might encounter. This model was designed to operate at the societal level and was not evaluated. Similarly, this study does not contribute to identifying the required components for constructing the intermediate Csa4Smms {RSA} framework; therefore, the study was not adopted.

The ninth study conducted by Potgieter et al. (2013) used browser integration to promote security values. In addition, this model provided security suggestions regarding specific user behaviour. This model could be accessed and used through the web browser. To utilise this model, a browser extension was developed to raise information security awareness by using a particular web browser such as Chrome, Firefox, Internet Explorer, Opera and Safari. The model was also evaluated. This model operated at organisational level and provided an interesting initiative. However, this model does not contribute to identifying components that can be adopted for constructing the intermediate Csa4Smms {RSA} framework; therefore, the study was not adopted.

The tenth study proposed an Information Security Retrieval and Awareness (ISRA) model to improve information security awareness for employees in the specific domain of industry (Kritzinger, 2006). This model consisted of the components such as “the ISRA dimensions (non-technical information security issues, IT authority levels and information security documents), information security retrieval and awareness, and measuring and monitoring” (Kritzinger & Smith, 2008, p224). This model focused completely on issues that were non-technical because this subject area was neglected compared to technical issues. It focused on an IT authority level to recognise various interested parties within the organisation and grouped them based on different IT authority levels that were similar across industries.

The ISRA model created a common body of knowledge by collecting and utilising national and international information from information security documents. This common body of knowledge was established to provide guidelines on how to secure information. In addition, the model used information security awareness to retrieve information from the ISRA dimensions. Furthermore, it enabled users to frequently

measure and monitor the latest ISA level in an organisation. This model provided a variety of required components to follow to construct an information security awareness model. The ISRA model operated at organisational level and was tested in an industry. Therefore, this model was adopted in the current study.

The eleventh study conducted by Moletsane and Tsibolane (2020) proposed a model which was constructed using the Knowledge, Attitude and Behaviour (KAB) model and the Theory of Planned Behaviour (TPB) in order to evaluate mobile information security for students in higher education. The model was proposed to operate at organisational level and evaluated through an explanatory study of a small sample of students in a higher educational institution in South Africa. However, this model was not adopted because it does not contribute to identifying the components that can be adopted for constructing the intermediate Csa4Smme {RSA} framework.

Based on the findings from the systematic literature review, none of the identified models and frameworks could be utilised completely and effectively for South African SMMEs without adjustments. The second sub-research question (SRQ2) was thus answered.

In conclusion, these adopted models and frameworks were analysed to identify certain building blocks that are required in constructing the intermediate Csa4Smme {RSA} framework. In addition, other studies included in Table 3-2 in the category “Designing and evaluating current awareness initiatives” will be analysed as well. Therefore, this study has identified the need to propose a framework that will promote cyber security awareness within South African SMMEs.

### **3.5 COMPONENTS FOR CYBER SECURITY AWARENESS FRAMEWORK**

This sub-section provides a discussion concerning components of a cyber security awareness framework as identified from the selected literature. Therefore, the sub-section addresses the third research question (SRQ3), namely:

*What components should be included in a cyber security awareness framework for SMMEs?*

Different researchers constructed security awareness models and frameworks following diverse approaches. As acknowledged in the literature study, components of cyber security awareness models or frameworks were identified as a way to structure awareness campaigns (Dlamini et al., 2011). These components were extrapolated from 29 studies identified through the systematic literature review and depicted in Figure 3-2. These studies were used to identify ten components to derive a common and complete list of components that could be utilised for the intermediate Csa4Smmes {RSA} framework. Eleven research studies proposed models and frameworks. Therefore, the identified common components are discussed based on a summary of the key aspects used in each model and framework that have been adopted and depicted in Table 3-5. In addition, six of the nine studies from the 29 studies, as shown in Table 3-2 in the category “Studies that focus on providing guidelines for cyber security awareness” were also included in the discussion to provide additional content regarding components (Dlamini & Modise, 2012; Kritzinger et al., 2017; Kritzinger et al., 2018; Labuschagne et al., 2011a; Lejaka et al., 2019; Von Solms, 2015).

However, not all studies provided a discussion concerning some of these components. Therefore, the discussion of each component is based on studies that have identified a particular component. The summary will be represented using tables that illustrate a comparison of words between models and frameworks that define a particular component.

The identified components are as follows:

- Clearly articulate goals and objectives.
- Appoint a dedicated team.
- Identify current training needs.
- Obtain support in the form of partnerships.
- Identify target audiences.
- Define topics to cover and their delivery methods.
- Establish a cyber security policy.



- Develop a strategy for implementation.
- Design an awareness and training strategy.
- Define evaluation methods.

### 3.5.1 Clearly articulate goals and objectives

Cyber security awareness goals and objectives should be defined following the “national legislation, laws, policies and standards as well as continental policies and agreements” (Dlamini et al., 2011, p27). These goals and objectives should be established in relation to a South African cyber security vision (Kritzinger et al., 2018), and they should be defined clearly (Kortjan & Von Solms, 2014). It is critical to ensure that any security-related awareness campaign should be designed according to and aligned with high-level security-related policies (Gundu & Flowerday, 2013a).

In addition, these goals can be used for tracking and evaluating the progress of an awareness programme over a specific period of time (Kritzinger, 2006). It is important for any cyber security awareness initiative to establish a plan that clearly defines its goals and objectives, including the expected results (Dlamini & Modise, 2012). This plan should assist SMMEs in setting basic cyber security goals (Bada & Nurse, 2019).

Table 3-6 focuses on a particular component in relation to goals and objectives.

**Table 3-6: Summary of the key aspects for goals and objectives**

<b>Clearly articulate goals and objectives</b>	Cyber security awareness goals and objectives should be defined (Dlamini et al., 2011).
	Cyber security awareness goals should be defined clearly (Kortjan & Von Solms, 2014).
	Cyber security awareness initiatives should be designed according to and aligned with the high-level goals, objectives and requirements of a cyber security policy (Gundu & Flowerday, 2013a).
	Goals and objectives can be used for tracking progress (Kritzinger, 2006).

	Basic security goals should be identified (Bada & Nurse, 2019).
--	---

The studies mentioned in Table 3-6 are aligned with one another because they all emphasise that a model or framework must clearly focus on the planned goals and objectives. These goals and objectives of the respective models must be defined clearly based on national legislation and policies. For this study, the term *Clearly articulate goals and objectives* has been adopted.

### 3.5.2 Appoint a dedicated team

A cyber security awareness framework recommends that a dedicated team or group such as government, private and public organisations and individuals be appointed (Kortjan & Von Solms, 2014). This dedicated team should be able to draft the comprehensive strategic plan (Kortjan, 2013) in order to enforce cyber security governance (Kritzinger, 2006). The team should also provide support in implementing the proposed cyber security awareness initiative (Dlamini et al., 2011; Dlamini & Modise, 2012). Moreover, the team will be responsible for planning and coming up with ways to govern cyber security awareness and usage of related technologies (Walaza et al., 2014). In addition, resources and services can be outsourced from trusted third-party organisations or individuals (Bada & Nurse, 2019). Table 3-7 focuses on a particular component in relation to appointing such a dedicated team.

**Table 3-7: Summary of the key aspects for appointing a dedicated team**

<b>Appoint a dedicated team</b>	Appointment of a dedicated team or group (Kortjan & Von Solms, 2014).
	Enforcement of cyber security governance (Kritzinger, 2006).
	Support from delegated teams and target audiences should be obtained (Dlamini et al., 2011).
	The delegated team should govern cyber security awareness and usage of ICT (Walaza et al., 2014).

	A trusted third-party organisation or individual with resources and services is required (Bada & Nurse, 2019).
--	--

Table 3-7 emphasises that the dedicated team must be selected to provide the intermediate Csa4Smmes {RSA} framework with the necessary support from a variety of people regardless of their job designations. In conclusion, the model should be supported by cyber security practitioners, community leaders, municipalities, company directors, law regulators and other trusted third-party contributors with the necessary resources and services (Bada & Nurse, 2019; Dlamini et al., 2011) to ensure there is a satisfactory cyber security awareness within SMMEs (Walaza et al., 2014). This dedicated team must be examined regularly for effectiveness and relevancy (Bada & Nurse, 2019). For the purposes of this study, the term *Appoint a dedicated team* has been adopted.

### 3.5.3 Identify current training needs

It is important to identify users' current levels of awareness regarding cyber security. Cyber security awareness topics should be aligned with preferred training (Dlamini et al., 2011; Kortjan & Von Solms, 2014). It is important for organisations to identify a problem at hand before conducting cyber security awareness (Gundu & Flowerday, 2013a). To develop a cyber security awareness initiative, a need assessment must be conducted to measure the current awareness level within the target audience (Kritzinger, 2006; Labuschagne et al., 2011a). This process ensures that training and awareness needs are relevant to the organisation's culture (Kritzinger, 2006). In addition, cyber security awareness initiatives must support the business needs of the organisation (Bada & Nurse, 2019). It is important to ensure that these needs are visualised and addressed through a collaborative effort by a community of cyber security (Kritzinger et al., 2018).

The cyber security awareness scope must be aligned with the organisational cyber security vision and mission because it is intended to make all users within the organisation conscious regarding the goals and objectives of the cyber security awareness programme. Organisations have special needs such as a tight budget, limitations of security knowledge, resources and security experts. Therefore, the scope

must consider external partners of the organisation. Table 3-8 focuses on a particular component in relation to identifying training needs.

**Table 3-8: Summary of the key aspects for identifying existing training needs**

<b>Identify current training needs</b>	“Identify current training needs” (Dlamini et al., 2011, p27).
	Preparation layer: handles the procedure of identifying the current level of awareness in cyber security (Kortjan & Von Solms, 2014).
	Measures current awareness level to identify any knowledge gaps (Gundu & Flowerday, 2013a).
	The retrieval of information will be required to determine cyber security awareness needs for relevancy (Kritzinger, 2006).
	Cyber security awareness initiatives must be aligned with the business needs of the organisation (Bada & Nurse, 2019).

As identified in Table 3-8, the above-mentioned studies define the process of identifying current training needs in different ways. The preparation layer handles the procedure of identifying the current cyber security awareness level. This preparation layer is concerned with defining resources to be offered by a cyber security awareness initiative to individuals within SMMEs. Such identification of the current needs helps in boosting the acceptance level of the proposed cyber security awareness framework. Furthermore, the term *Identification of current training needs* has been adopted for this study.

#### **3.5.4 Obtain support in the form of partnerships**

Cyber security awareness should be supported by a variety of parties, including the cyber security departments of organisations, community leaders, management and other law regulators (Dlamini et al., 2011; Kritzinger, 2006). The approval or rejection of the implementation of cyber security awareness model or framework should be identified in conjunction with potential support to enhance the probability of approval.

Partnerships should be established because it is mandatory for management to endorse, support and commit to ongoing cyber security awareness programmes and initiatives. By obtaining support from management, the partnership will ensure that cyber security awareness programmes and initiatives are implemented successfully within the organisation. In addition, these partnerships reduce the complexity of obtaining support regarding the needed resources (Kortjan & Von Solms, 2014; Kritzinger et al., 2017). Employees are likely to comply if the requirements are prescribed by management. Therefore, these trusted partnerships must be maintained. These partnerships must be established with all cyber security collaborators, including industry and academia (Kritzinger et al., 2017; Kritzinger et al., 2018). Table 3-9 focuses on a particular component in relation to forming partnerships.

**Table 3-9: Summary of the key aspects for forming partnerships**

<b>Obtain support in the form of partnerships</b>	Obtain support from a variety of parties, including management and government for successful implementation (Dlamini et al., 2011).
	Obtaining management support helps to set the direction for cyber security policies and procedures to enhance their probability of approval (Kritzinger, 2006).
	Partnerships should be established for successful implementation (Kortjan & Von Solms, 2014).
	Partnerships with trusted third parties must be established and maintained (Bada & Nurse, 2019).

As identified in Table 3-9, it is important to form partnerships with various stakeholders to gain the necessary support from them. These partnerships can help with encouraging all cyberspace users to participate in and contribute to the goals of the intermediate Csa4Smmes {RSA} framework. In addition, the term *Obtain support in the form of partnerships* has been adopted for this study.

### 3.5.5 Identify target audiences

The cyber security awareness audiences are organisations and individuals who will receive knowledge from the proposed awareness programmes. Cyber security awareness should reach out to multiple internet users within SMMEs, including employees, employers and other external individuals associated with SMMEs to enlighten them regarding cyberspace (Dlamini et al., 2011). In addition, the intended target audience, including management, IT or security staff and internet users, needs to be identified, grouped and addressed independently to make the awareness programme more effective. Cyber security awareness content must be formulated based on the target audience so that it can be balanced because if the message is not easy to understand, novice users will lose interest, whereas if an easy message is presented, professionals will be bored. Target audiences can be defined and divided according to their current security knowledge (Kortjan & Von Solms, 2014). Table 3-10 focuses on a particular component in relation to the identification of target audiences.

Table 3-10: Summary of the key aspects for identifying target audiences

<b>Identify target audiences</b>	Identify intended audiences (Dlamini et al., 2011).
	The delivery layer helps with defining the target audience (Kortjan & Von Solms, 2014).

The intermediate Csa4Smmes {RSA} framework should cater for a variety of target audiences. The term *Identify target audiences* has been adopted for the purposes of this study.

### 3.5.6 Define topics to cover and their delivery methods

A method for delivering cyber security awareness should be chosen based on the topic, content and medium (Kortjan & Von Solms, 2014), meaning that a selected delivery tool will influence the proposed awareness topic, content and medium. Cyber security awareness topics must be evaluated for relevance according to target audiences (Dlamini et al., 2011). These topics should be universal, relevant, diverse

and tailored to a variety of target audiences (Gundu & Flowerday, 2013a). For instance, management users do not have enough time to pay attention to and focus on unnecessary details.

However, a cyber security awareness topic can be presented by using a variety of delivery methods to provide different cyber security awareness content. This content ensures that the utilised delivery materials are well-accepted and the delivered information well-interpreted by the target audience. Cyber security awareness content can be established based on organisational internal cyber security policy, international cyber security standards, action plans and common cyber security mistakes made by employees.

Organisations can develop action plans to address the desired cyber security related risks (Bada & Nurse, 2019). Therefore, when developing cyber security awareness material, the topics and delivery methods must be dependent on the needs assessments. In addition, the choice of techniques to be implemented will also be dependent on resources and the complexity of the messages to be delivered (Labuschagne et al., 2011a). Table 3-11 focuses on a particular component in relation to topics to cover.

**Table 3-11: Summary of the key aspects for defining topics to be covered**

<b>Define topics to cover and their delivery methods</b>	Preparation layer: A suitable tool for delivering awareness should be chosen (Kortjan & Von Solms, 2014).
	Define topics to be covered and methods to be used (Dlamini et al., 2011).
	Awareness topics should be universal and diverse (Gundu & Flowerday, 2013a).
	Develop action plans to address the desired cyber security related risks (Bada & Nurse, 2019).

The selected list of awareness topics must be evaluated based on compatibility with the identified target audience. Kortjan and Von Solms (2014) state that the preparation

layer consists of four sub-components, namely topics, content, medium and tools. Therefore, this study uses the term *Define topics to cover and their delivery methods* as a component name.

### 3.5.7 Establish a cyber security policy

A cyber security policy provides guidelines and procedures that must be followed to govern all cyber security related situations (Dlamini et al., 2011). Organisations must establish an up-to-date cyber security policy that is in line with international standards (Dlamini et al., 2011; Gundu & Flowerday, 2013a; Kritzinger, 2006). It is mandatory for organisations to evaluate and upgrade their internal cyber security policy based on international standards (Gundu & Flowerday, 2013a). The action plan for a cyber security awareness framework should be outlined (Kortjan & Von Solms, 2014). The intermediate Csa4Smme {RSA} framework must follow a national plan to describe the process that will improve cyber security awareness for individuals within SMMEs. In addition, the intermediate Csa4Smme {RSA} framework must provide efficient support to ensure that cyber security policies are implemented (Kritzinger et al., 2017) to govern the usage of cyber security related resources within organisations (Walaza et al., 2014). Table 3-12 focuses on a particular component in relation to establishing a cyber security policy.

**Table 3-12: Summary of the key aspects for establishing a cyber security policy**

<b>Establish a cyber security policy</b>	Establish and implement a cyber security policy (Dlamini et al., 2011; Kritzinger, 2006).
	Ensure the existence of an up-to-date cyber security policy by evaluating and upgrading the policy regularly (Gundu & Flowerday, 2013a).
	The strategic layer: The cyber security awareness action plan should be outlined (Kortjan & Von Solms, 2014).
	Develop a cyber security policy and standards to govern the usage of cyber security related resources (Walaza et al., 2014).



As identified in Table 3-12, the strategic layer reflects the overall vision of government and the organisation regarding cyber security awareness. This layer helps with planning strategies for approaching cyber security awareness. In addition, establishing a cyber security policy helps with the process of controlling all cyber security related assets. In this study, the term *Establish a cyber security policy* has been adopted.

### 3.5.8 Develop a strategy for implementation

The implementation strategy for cyber security awareness should be developed to evaluate the programme for all potential ambiguities (Dlamini et al., 2011). To guarantee a well-timed execution, the design and implementation strategy should be prepared while considering the accessibility of staff and other businesses, including financial resources (Gundu & Flowerday, 2013a). An action plan must be outlined (Kortjan & Von Solms, 2014) to verify that policies and procedures are implemented and enforced (Kritzinger, 2006). In addition, this plan must deal with security-related issues (Bada & Nurse, 2019). The tailored content for a specific target audience, its applicable delivery and evaluation methods and other business priorities should be planned and implemented accordingly. It is important to specify the implementation plan and the evaluation method to be used when measuring for effectiveness (Dlamini & Modise, 2012). Table 3-13 focuses on a particular component in relation to strategies for implementation.

**Table 3-13: Summary of the key aspects for developing a strategy for implementation**

<b>Develop a strategy for implementation</b>	Develop a strategy for implementation (Dlamini et al., 2011).
	An action plan should be outlined to ensure that the design and implementation of awareness initiatives are defined properly (Gundu & Flowerday, 2013a; Kortjan & Von Solms, 2014).
	Confirm the implementation and enforcement of cyber security policies and procedures in order to deal with security issues (Bada & Nurse, 2019; Kritzinger, 2006).

The implementation plan should be developed to outline the approach to cyber security awareness. This plan must consist of clear processes to be followed, their timelines, the recent progress status and the responsible team. This plan must be drafted because it helps to clarify how strategies should be followed cornering the approach to cyber security awareness. Therefore, this study has adopted the term *Develop a strategy for implementation*.

### 3.5.9 Design an awareness and training strategy

Cyber security awareness strategies should be developed to attract and retain an audience (Dlamini et al., 2011). Similarly, a training strategy is important because it helps with handling all arrangements concerning how and where training will be provided. A cyber security awareness campaign should be clearly defined and the required resources must be allocated to awareness and training (Gundu & Flowerday, 2013a). Essential resources for all identified layers should be in place (Kortjan & Von Solms, 2014), including finances to implement and maintain awareness measures (Kritzinger, 2006). These resources are required to establish good policies and standards (Walaza et al., 2014). Table 3-14 focuses on a particular component in relation to designing awareness and training strategies.

**Table 3-14: Summary of the key aspects for designing strategies for awareness and training**

<b>Design an awareness and training strategy</b>	Design an awareness and training strategy (Dlamini et al., 2011).
	Resources (financial, facilities, human capacity and others) should be in place and allocated to awareness and training (Gundu & Flowerday, 2013a; Kortjan & Von Solms, 2014).
	Provide financial resources to implement and maintain awareness measures (Kritzinger, 2006).
	Resources are required to formulate good policies and standards (Walaza et al., 2014).

Within each identified layer of the intermediate Csa4Smmes {RSA} framework a set of appropriate resources are required to be in place for those layers to be addressed.

Strategies must be identified to ensure that audiences are attracted and kept attentive. These strategies ensure the alignment of the trainer, audience, venue and other essential resources. For the purposes of this study the term *Design an awareness and training strategy* has been adopted.

### 3.5.10 Define evaluation methods

Methods for evaluating cyber security awareness must be identified and developed to assess and measure their effectiveness (Dlamini et al., 2011). In addition, evaluation is important because it provides feedback to measure the success and the effectiveness of the intermediate Csa4Smmes {RSA} framework (Gundu & Flowerday, 2013a), to identify benefits or drawbacks, to determine the quality of the adaptation of the framework and to identify room for improvement (Dlamini & Modise, 2012; Labuschagne et al., 2011a).

Controls to measure and monitor progress must be prepared to ensure effective communication with audiences (Walaza et al., 2014). Monitoring helps in ensuring that new security problems and other related documentations are integrated into the intermediate Csa4Smmes {RSA} framework (Kritzinger, 2006). These monitoring techniques should be defined (Kortjan & Von Solms, 2014) in order to regularly re-examine trusted third parties (Bada & Nurse, 2019). Evaluation provides feedback concerning the failure or effectiveness of the intermediate Csa4Smmes {RSA} framework, while monitoring helps in keeping track of activities within the intermediate Csa4Smmes {RSA} framework. Table 3-15 summarises the components in relation to developing evaluation methods.

**Table 3-15: Summary of the key aspects for defining evaluation methods**

<b>Define evaluation methods</b>	Develop evaluation methods (Dlamini et al., 2011).
	It is important to measure a framework to determine its success (Gundu & Flowerday, 2013a).
	Controls to measure and monitor must be prepared to ensure effective communication with audiences (Walaza et al., 2014).

	The monitoring helps in ensuring that new security problems and related documentations are integrated into the framework (Kritzinger, 2006).
	Monitoring techniques should be defined (Kortjan & Von Solms, 2014).
	Regularly re-examine trusted third parties (Bada & Nurse, 2019).

As emphasised in Table 3-15, it is important for the intermediate Csa4Smms {RSA} framework to establish a set of processes to evaluate cyber security awareness initiatives and programmes. Evaluation methods are concerned with testing the effectiveness of cyber security awareness, using a variety of tools such as comparing preliminary and post surveys. In addition, the intermediate Csa4Smms {RSA} framework should be evaluated for effectiveness and improvement. For this study, the term *Define evaluation methods* has been used.

### **3.5.11 Ten components of a cyber security awareness framework**

As discussed in this chapter, common components were identified and represented in a graphical representation as shown in Figure 3-4.



Figure 3-4: Components of a cyber security awareness framework for SMMEs (Lejaka et al., 2019)

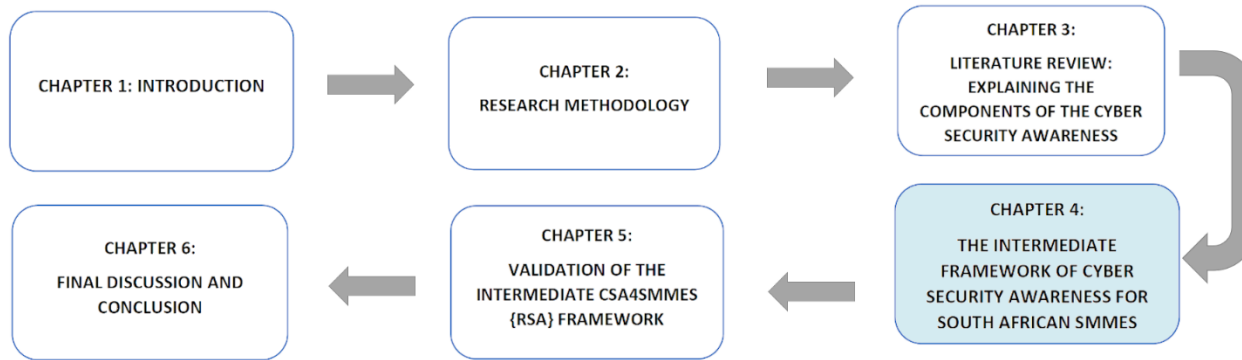
### 3.6 SUMMARY

Based on systematic literature review findings, a research gap has been identified whereby a cyber security awareness study has not been conducted for South African SMMEs where a suitable model and framework for raising cyber security awareness for SMMEs in South Africa have been developed. However, eleven models and frameworks were evaluated to identify components of the intermediate Csa4Smms {RSA} framework. Therefore, the common components, as illustrated by Figure 3-4, was used as building blocks when developing the intermediate Csa4Smms {RSA} framework.

This chapter answered the third sub-research question (SRQ3) because components to be included in the intermediate Csa4Smms {RSA} framework were identified as shown in Figure 3-4. The first sub-research question (SRQ1) and second sub-research question (SRQ2) were also answered.

The next chapter focuses on the development of the intermediate Csa4Smmes {RSA} framework.

# CHAPTER 4: THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY AWARENESS FOR SOUTH AFRICAN SMMEs



<b>CHAPTER 4: INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK</b>	4.1	INTRODUCTION	4.2	OVERVIEW OF CHAPTER 4
	4.3	BUSINESS CHARACTERISTICS OF SOUTH AFRICAN SMMEs	4.4	THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK
	4.5	SUMMARY		

# 4 THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY AWARENESS FOR SOUTH AFRICAN SMMEs

## 4.1 INTRODUCTION

This chapter proposes the intermediate framework of cyber security awareness for South African SMMEs which will be identified as the intermediate Csa4Smme {RSA} framework. The chapter also addresses the following research questions:

- *SRQ4: What are the cyber security awareness needs within the South African community of SMMEs from a literature perspective?*
- *SRQ5: What would the intermediate Csa4Smme {RSA} framework comprise for the South African community of SMMEs?*

Figure 4-1 highlights the second phase of the DSRM process to be followed by the study.

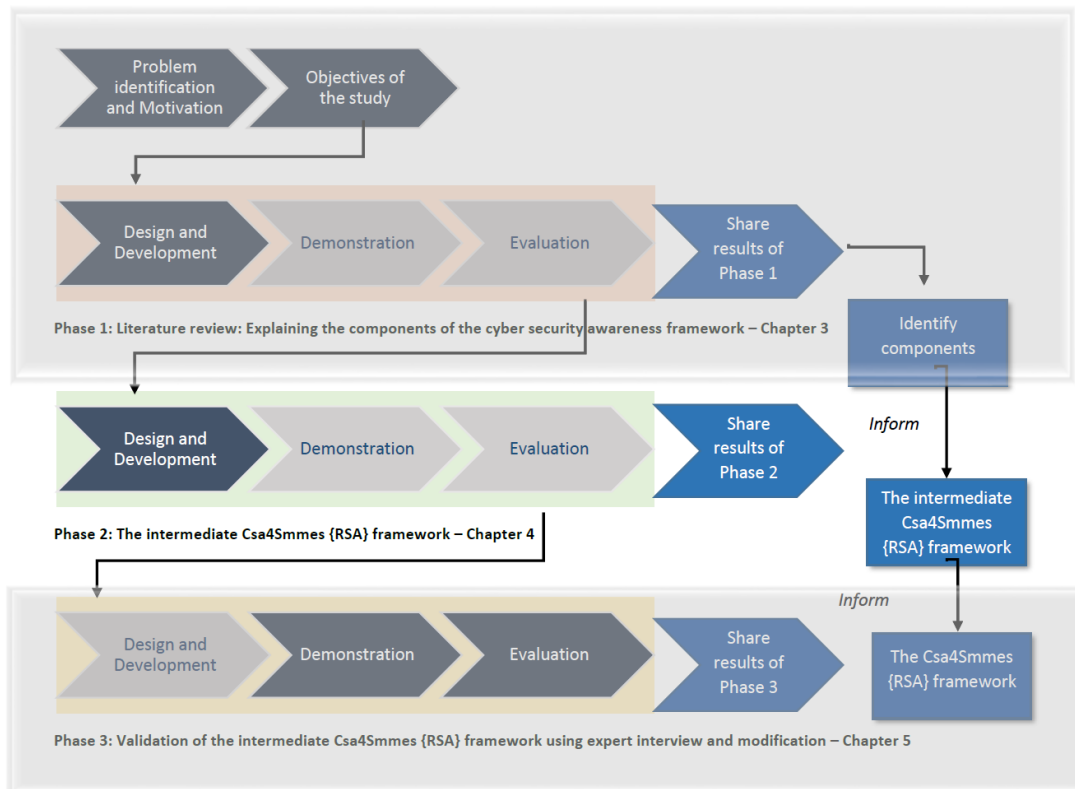


Figure 4-1: DSRM Process - Phase 2: The development of the intermediate Csa4Smme {RSA} framework



The chapter is presented as the second phase as shown in Figure 4-1. This phase concentrates on developing the intermediate Csa4Smmes {RSA} framework. In this phase, the selection of appropriate cyber security awareness components that are suitable for SMMEs are highlighted. However, a general background is initially provided to discuss the business characteristics of South African SMMEs.

## **4.2 OVERVIEW OF CHAPTER 4**

Chapter 4 begins with a discussion regarding business characteristics of South African SMMEs (Section 4.3) to align the development of the intermediate Csa4Smmes {RSA} framework with these characteristics. A discussion regarding the development of the intermediate Csa4Smmes {RSA} framework is presented in Section 4.4. The summary of the research chapter is provided in Section 4.5.

## **4.3 BUSINESS CHARACTERISTICS OF SOUTH AFRICAN SMMEs**

This sub-section aims to study SMMEs by highlighting their phases of development, unique business characteristics, importance, reliance on IT, and challenges and requirements for cyber security. The sub-section addresses the fourth sub-research question (SRQ4):

*What are the cyber security awareness needs within the South African community of SMMEs from a literature perspective?*

### **4.3.1 Defining SMMEs**

There is no common and official way of defining a small business (Andreassen, 2011; Coetzer, 2015; Sami, 2016; Scarborough & Zimmerer, 2006; Smit & Watkins, 2012). Small businesses depend on certain characteristics such as being self-sufficiently owned, managed, funded and operated by one or a very few people. Usually, small businesses (SMMEs in the South African context) manage company operations by using an informal management structure (Nieman & Nieuwenhuizen, 2014). They can be run by a single employee or entrepreneur attempting to build a company for their own survival, mainly in the early stage of the business. SMME owners may have inadequate skills and

knowledge to purposefully grow and manage their enterprises (South African Institute of Chartered Accountants, 2015). Their enterprises usually have a reasonably smaller market share (Beaver, 2007; Sami, 2016).

Based on this discussion, the process of constructing the intermediate Csa4Smme {RSA} framework considered the fact that SMMEs are different from large companies. In addition, these SMMEs must be provided with tailored cyber security awareness based on company size, field of operation as well as in-house skills and resources.

### 4.3.2 Phases of SMME development

In South Africa, the National Small Business Amended Act No. 102 of 2004 views an SMME as “a separate and distinct business entity, including co-operative enterprises and non-governmental organisations, which is managed by one or more owner(s), which predominantly conducts its business in any sector or subsector of the national economy” (South Africa, 2004, p3). Organisations, including SMMEs, progress in different phases. Figure 4-2 describes the five phases of SMME development (Lewis & Churchill, 1983).

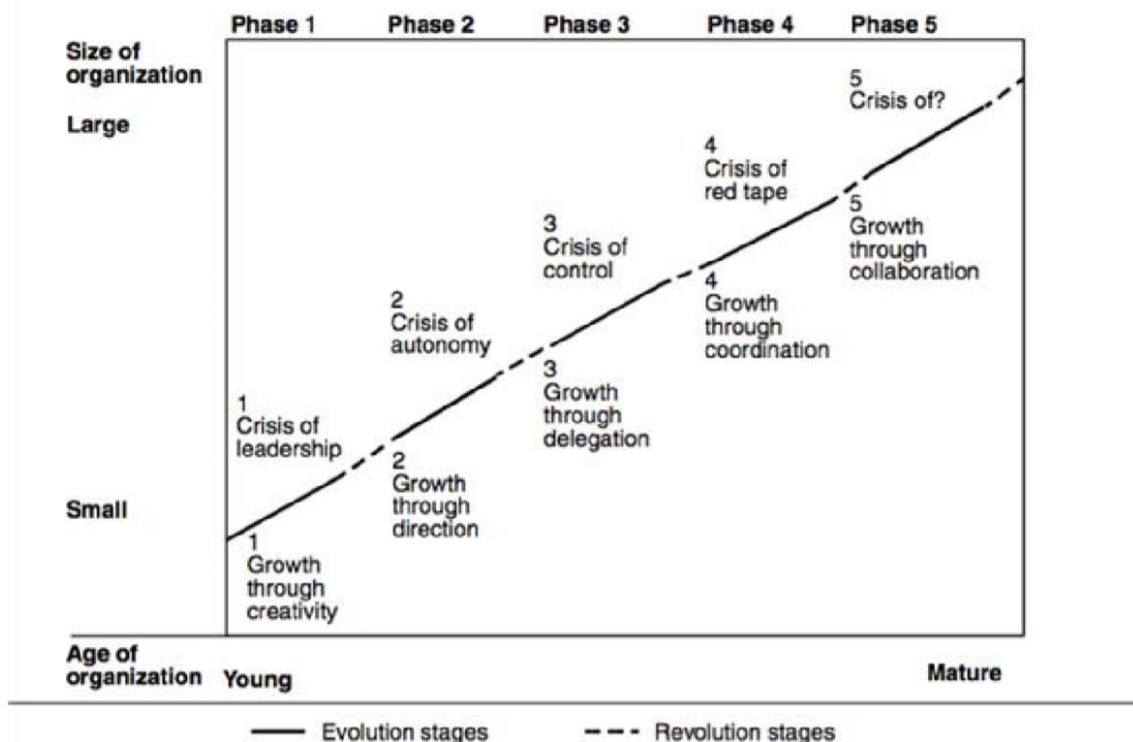


Figure 4-2: Five phases of SMME development (Lewis & Churchill, 1983)

The first phase of SMME development (“Growth through creativity”) is when the owner utilises his skills and knowledge to establish a business. The second phase (“Growth through direction”) is when the owner manages to hire more employees to help with producing and selling products and services. The third phase (“Growth through delegation”) is when the owner can delegate work to employees and still sustain the business itself. The fourth phase (“Growth through coordination”) is when the owner can provide guidance to employees. The last phase of SMME development (“Growth through collaboration”) is when an SMME can manage without involvement of the owner. These phases shows that an SMME has matured into an organisation (Lewis & Churchill, 1983).

In addition, the National Small Enterprise Act No. 102 of 1996 categorises SMMEs into five different categories (Lewis & Churchill, 1983). They are as follows:

1. *Survivalist enterprises (Existence stage)*: In a survivalist enterprise, there is an individual owner with minimal training and asset investment (Fani, Von Solms, & Gerber, 2017). In general, this enterprise has no compensated workers and usually generates income lower than the minimum income standard (Upfold, 2005). Furthermore, survivalist enterprises operate in the informal sector of the economy (Fani et al., 2017).
2. *Micro-enterprises (Survival stage)*: In micro-enterprises, usually there are less than five compensated workers. This enterprise lacks formal management in order to handle processes such as tax registration, labour legislation, business premises and accounting procedures. A micro-enterprise is an informal enterprise without formal business infrastructure (Fani et al., 2017). In addition, both survivalist and micro-enterprises usually do not have internal cyber security skills (Upfold, 2005) and usually have basic business skills.
3. *Very small enterprises (Success stage)*: A very small enterprise usually consists of less than ten paid employees and at this stage the enterprise is stable (Fani et al., 2017). The owner formally registers the enterprise to operate in the formal sector of the economy. This enterprise usually has access to modern technology; however, it lacks cyber security awareness (Upfold, 2005). This enterprise must

conduct research to ensure sustainability with the limited resources the business currently has (Fani et al., 2017).

4. *Small enterprises (Take-off stage)*: The small enterprise usually has the capacity to employ approximately 100 employees and can run without the owner managing the enterprise. However, the owner's guidance is required (Fani et al., 2017). Small enterprises usually have fixed business premises and they also have sophisticated information systems. However, small enterprises often lack cyber security.
5. *Medium-sized enterprises (Resource mature stage)*: The medium-sized enterprise usually has the capacity to employ approximately 200 employees. In this phase, medium-sized enterprises can manage without the owners' involvement (Fani et al., 2017). Medium-sized enterprises operate from a fixed infrastructure and are regarded as well-established enterprises.

SMMEs can go through all the different phases of development, starting as a survivalist enterprise at the existence stage until they become medium-sized enterprises at the resource matured stage. Through these phases, SMMEs can develop into successful organisations with structured management and financial stability. Therefore, the intermediate Csa4Smmes {RSA} framework supported SMMEs through the different phases of development.

Furthermore, the framework included non-governmental organisations that fall within the category of very small enterprises, small enterprises and medium-sized enterprises (ranging from phase 2 to phase 5 of SMME development as indicated in Figure 4-2). These types of organisations are included because they depend on IT to grow and sustain the businesses. However, they do not have sufficient resources to deal with cyber security issues.

Certain characteristics of SMMEs are discussed in the next sub-section.

### 4.3.3 Characteristics of SMMEs

SMMEs and large organisations share particular characteristics; however, SMMEs also have their unique characteristics (Sami, 2016; Stokes & Wilson, 2010). SMMEs are increasingly relying on IT to store confidential and valuable information within their systems, including personal and credit card information of customers, clients and patients (Von Solms, 2015). SMMEs are frequently linked to larger enterprises in terms of providing services and products. This relationship can be an opportunity for criminals to launch a cyber security related attack against larger enterprises (Von Solms, 2015).

SMMEs regardless of industry, share several characteristics, including the following (Andoh-Baidoo, Osatuyi, & Kunene, 2014; Beaver, 2007; Beaver & Jennings, 2005; Mahadea & Pillay, 2008; Nieman & Nieuwenhuizen, 2014; Sami, 2016; Stokes & Wilson, 2010):

- *Independent and owner-managed:* SMMEs are typically managed by the owner. In addition, they can also be managed by a sole manager employed by the owner.
- *Level of resource constraints:* SMMEs encounter numerous limitations concerning resources in terms of technical, financial and human capacity. The main constraint for SMME growth is access to financial resources.
- *Limited product range:* SMMEs are constraint to provide products and services at a certain level.
- *Not dominant in their field:* Due to their size SMMEs are often not leaders in the field of their business operations.

Furthermore, SMMEs have other characteristics in relation to their size, geographical location, type of ownership, economic growth, business development and technique of managing the business (Coertze, 2012; Devos, Landeghem, & Deschoolmeester, 2012). These SMME characteristics were considered while developing the intermediate Csa4Smmes {RSA} framework because SMMEs must be provided with a tailored cyber security awareness content which is aligned with the characteristics discussed above. In

addition, these characteristics are incorporated into the intermediate Csa4Smmes {RSA} framework to ensure that cyber security needs of South African SMMEs are identified and addressed.

The next sub-section discusses the importance of SMMEs.

#### **4.3.4 Importance of SMMEs in a country**

SMMEs form the most important share of the economy across the world (Sánchez, Ruiz, Fernández-Medina, & Piattini, 2010). Countries and economies depend on SMMEs for innovation and flexibility to make unique economic contributions (Coertze, 2012; Le Roux, 2010; Koornhof, 2009). Therefore, SMMEs are regarded as contributors to economic growth and they assist in reducing poverty by creating essential employment for unemployed individuals (Abor & Quartey, 2010; Dhillon, Stahl, & Baskerville, 2009). SMMEs in general are considered the mainspring of creating jobs, improving the economy and reducing poverty in developing countries (Sami, 2016; Nichter & Goldmark, 2009).

In South Africa, SMMEs comprise a significant share of the economy and they must be protected properly to ensure their sustainability (Van De Haar, 2014). In summary, SMMEs are regarded important based on the following reasons (Coertze, 2012; Megginson, Byrd, & Megginson, 2006):

- SMMEs provide employment opportunities for citizens more than other sized organisations.
- SMMEs are potential competitors of larger organisations; therefore, they are keeping larger organisations competitive.
- SMMEs inspire flexibility and innovation.
- SMMEs offer a variety of opportunities to inspire entrepreneurs who are unemployed, underemployed or retrenched.
- SMMEs provide employees with limited or no skills and training a comprehensive learning experience.

- SMMEs operate more closely with communities and their customers.

SMMEs enhance the economy of a country and in South Africa, there is a significant increase in the number of SMMEs (Kent et al., 2016). However, SMMEs are not prepared effectively to deal with cyber security issues (PwC, 2016). Therefore, the intermediate Csa4Smmes {RSA} framework provides support for SMMEs to enhance the level of cyber security awareness within their organisations because they depend on IT resources for effective business operations.

#### **4.3.5 Information technology dependency**

SMMEs are gradually becoming more dependent on information technology (IT) which enables them to connect with other parties throughout the world. IT assists SMMEs in reaching out to broader markets (Van De Haar, 2014). It is important for SMMEs to be up-to-date with modern technology in order to be relevant within the market and also to retain customers (Sami, 2016).

SMMEs utilise available communication tools such as smartphones to improve their operations, including customer service and productivity for both employees and customers (Van De Haar, 2014). Furthermore, using such communication tools could assist SMMEs in reducing limited budgets and costs linked to resources (Fani et al., 2017). In SMMEs, management personnel use IT as a key tool to ensure operational benefits and business growth (Van De Haar, 2014). SMMEs can no longer ignore IT because they are dependent on it to perform everyday business operations (Van De Haar, 2014).

In addition, SMMEs depend increasingly on information systems which consist of a well-integrated computer hardware, software, data, people and procedures (Upfold, 2005). These SMMEs become increasingly connected to the internet and rely on it to do business (Von Solms, 2015). However, cyber security continues to be a challenge which is regularly viewed as unapproachable and difficult for SMMEs to address (Coertze, 2012; Gupta & Hammond, 2005; Upfold & Sewry, 2005). SMMEs often consider larger

organisations to be more at risk from security incidents than themselves (Coertze, 2012; Rees, 2010).

As discussed, IT plays a significant role in daily operations within SMMEs. However, they do not recognise that it is important to handle cyber security from within (Von Solms, 2015). There are certain challenges that SMMEs encounter which might influence their development and their ability to protect themselves against cyber attacks. These challenges are discussed in the next sub-section.

#### **4.3.6 Challenges faced by SMMEs**

SMMEs are vulnerable to cyber attacks and lack cyber security measures (PwC, 2020). SMMEs are increasingly targeted by cyber criminals (Bedi, 2013; Hubbard, 2019; Microsoft, 2019; Morgan, Colebourne, & Thomas, 2006; Park, Robles, Hong, Yeo, & Kim, 2008; Symantec, 2019). SMMEs should protect themselves against cyber attacks because that may result in their becoming a growing cyber risk to themselves, their clients, other organisations (in collaboration with) and the country as a whole (Von Solms, 2015).

Furthermore, legal developments in South Africa such as the POPI Act may pressurise SMMEs to establish or upgrade their cyber security instruments because the POPI Act requires that organisations protect information about their clients, customers and other individuals. The Act applies to public and private entities, and according to condition 7 relating to security, SMMEs would entail implementing security controls in cyberspace (POPI Act, 2013). This Act requires SMMEs to be responsible for protecting data for integrity and confidentiality. Therefore, SMMEs must identify reasonable internal and external cyber security risks, and identify, implement and evaluate measures to encounter the identified risks. SMMEs must establish cyber security standards, practices and procedures to be followed within their organisation.

The intermediate Csa4Smmes {RSA} framework will help SMMEs to be compliant with certain aspects of condition 7 of the POPI Act. As SMMEs increasingly develop in size, the complexity of doing business increases as well (Upfold, 2005). The development of



SMMEs is typically constrained through limited financial resources and expertise. They perhaps do not have adequate internal IT experts (Upfold, 2005) and they find it challenging to develop adequate cyber security measures due to a shortage of finance and technical resources (PwC, 2020; Harris & Patten, 2014; Von Solms, 2015). SMMEs encounter problems in implementing cyber security policies and are often not prepared to deal with increasing cyber security related issues (Bedi, 2013). In addition, they do not have a desire to spend more on security applications which makes them easy targets for hackers (Bedi, 2013).

In conclusion, several challenges encountered by SMMEs, particularly SMMEs in South Africa, are as follows (Fani et al., 2017; Soni, Cowden, & Karodia, 2015):

- *Education and skills:* Often, SMME owners do not have adequately skills for business operations and management (SAICA, 2015). They do not have enough understanding and capability that are mostly acquired through learning from educational institutions and industrial exposure (Fani et al., 2017). SMME owners, when establishing a business, may not include business operational documentation, finance and general management in their business strategy (Sami, 2016).
- *Location:* The geographical location plays a significant role in the success of SMMEs. A good geographical location contributes to attracting and retaining clients (Fani et al., 2017). SMMEs often use their households as their initial office space; alternatively they occupy any cost-effective geographical location (Coertze, 2012). Therefore, SMMEs will have difficulty in expanding their business and reaching certain figures in terms of clients and revenue.
- *Registration:* Most SMMEs are not registered because they are typically too small to operate officially (Fani et al., 2017). However, those SMMEs that can register may have a challenge in sustaining the registration because the annual-based procedures and processes can be expensive for SMMEs (Soni et al., 2015).
- *Tax:* All registered organisations, including SMMEs, are liable to pay tax to the

South African Revenue Service (SARS) in the context of this study (Fani et al., 2017). In this case, SMMEs are obligated to pay tax and if payment is not made, there can be penalties and fines towards that organisation.

- *ICT*: ICT is a vital resource which all organisations should have and utilise effectively. However, SMMEs do not have enough budget to purchase the required ICT resources (Von Solms, 2015). On the other hand, large organisations have a dedicated team of people handling ICT-related issues such as information security incidents and attacks, hardware and network issues (Fani et al., 2017). However, many SMMEs do not have adequate financial support to afford such IT departments (Von Solms, 2015). Moreover, lack of knowledge of how to utilise ICT effectively can prevent SMMEs from integrating ICT into their daily business operations (Soni et al., 2015).

Based on the discussion above, it is important for the intermediate Csa4Smme {RSA} framework to ensure that all SMMEs receive tailored cyber security awareness regardless of their challenges. This discussion emphasises that SMMEs often encounter several challenges which could affect their daily business operations.

These challenges contribute to the high rates of SMME failure in running a business effectively (Smit & Watkins, 2012). Some of these challenges may include lack of staff, business processes, technology and specialised knowledge (Coertze, 2012). In conclusion, SMMEs specifically in South Africa, frequently struggle to implement and maintain cyber security (Upfold & Sewry, 2005). Therefore, when developing the intermediate Csa4Smme {RSA} framework, these identified challenges and characteristics were considered to meet the needs of South African SMMEs. Therefore, the selected challenges and characteristics are summarised as follows:

- *Independently owned*: SMMEs are owned by one or a few people compared to large organisations.
- *Resource constraints*: SMMEs often do not have adequate financial, technical, specialist or human capacity resources required to effectively develop sustainable

cyber security infrastructure.

- *Limited education towards business management and compliance (POPI Act):* Many SMMEs lack awareness of current cyber security trends and relevant legal developments.
- *Poor implementation and maintenance of cyber security:* SMMEs frequently do not have adequate resources to implement and maintain cyber security infrastructure.
- *Vulnerability to cyber attacks:* SMMEs are dependent on IT; however, they are vulnerable to cyber security related attacks.
- *Dependency on IT:* SMMEs depend on IT for successful business operations, and to attract and retain customers.
- *Close operations with large organisations, communities and their customers:* SMMEs can store and access confidential information of individuals, people in communities and large companies. However, SMMEs do not have the required resources to protect such confidential information.
- *Bad geographical location:* SMMEs are normally situated in a location which is not suitable for business. Therefore, they may have limited access to the required resources to establish and maintain cyber security infrastructure.

In conclusion, these identified challenges and characteristics will be considered when developing the intermediate Csa4Smmes {RSA} framework to enhance the level of cyber security awareness within South African SMMEs. These aspects must be incorporated because SMMEs face different challenges as discussed. Therefore, the intermediate Csa4Smmes {RSA} framework must provide support for all SMMEs regardless of characteristics and challenges.

The next sub-section provides an overview of components that are required to build the intermediate Csa4Smmes {RSA} framework which is tailored for South African SMMEs.

## 4.4 THE INTERMEDIATE CSA4SMMES {RSA} FRAMEWORK

A variety of components of the intermediate Csa4Smmes {RSA} framework have been identified in Chapter 3. Therefore, this section aims to identify, refine and combine relevant components of the intermediate Csa4Smmes {RSA} framework. Furthermore, the chapter aims to develop the intermediate Csa4Smmes {RSA} framework that is relevant for SMMEs.

The sub-section mainly addresses the fifth sub-research question (SRQ5):

*What would the intermediate Csa4Smmes {RSA} framework comprise for the South African community of SMMEs?*

The intermediate Csa4Smmes {RSA} framework is developed by incorporating identified cyber security awareness components as depicted in Chapter 3, Figure 3-4.

This intermediate Csa4Smmes {RSA} framework is developed to support the South African government's responsibility of promoting cyber security awareness within the country (Grobler, Van Vuuren, & Leenen, 2012). Therefore, the intermediate Csa4Smmes {RSA} framework is constructed through findings from the systematic literature study. The following section discusses components as identified from the previous chapter. In addition, four high-level stages of the National Institute of Standards and Technology (NIST) framework, as cited by Labuschagne et al. (2011a), will be used.

In conclusion, all identified components are utilised to construct the intermediate Csa4Smmes {RSA} framework. The intermediate Csa4Smmes {RSA} framework for SMMEs specifically in South Africa is discussed further in the next sub-section. However, it is important to discuss different types of frameworks that can be developed in the context of this study.

### 4.4.1 Introduction

A model is a simplified way of presenting identified problems and future solutions in a schematic form. A model can also be referred to as a concept and illustration of a problem or solution which might include frameworks and guidelines (Vaishnavi & Kuechler, 2015).

On the other hand, a framework can be defined as a layout to represent the design of new systems or products (Coertze, 2012). Therefore, this study develops a framework for raising cyber security awareness within the community of South African SMMEs. In addition, a framework can be defined as a skeleton structure aimed to protect or enclose something (Robinson, 2013), and the following list presents the different types of frameworks (Eisenhart, 1991):

- *Theoretical framework*: The theoretical framework is mainly designed to support the theory of research. This framework is a collection of theories that are assembled to lay out a foundation or assist in explaining, viewing or formulating a phenomenon (Labaree, 2013).
- *Practical framework*: The practical framework does not depend on formal theory; however, it depends on the collected practice knowledge of experts, outcomes from previous research and regularly the perspectives presented as a result of public view (Eisenhart, 1991).
- *Conceptual framework*: A conceptual framework is a type of framework for justifications since it can analyse different views and deliver a conclusion based on various reasons for adopting a point. Eisenhart (1991) additionally states that a conceptual framework is based on prior research and literature, and it is constructed from a collection of present and far-ranging sources. In addition, a conceptual framework can also be defined as a written or graphical representation that provides details about certain things to be studied and recognise relationships among them (Miles & Huberman, 1994).

In conclusion, the difference between the theoretical and conceptual framework is provided. The theoretical framework provides an explanation on conception that is related to the phenomenon, while a conceptual framework is a design that best describe the conception taken from a specific phenomenon (Camp, 2001). As a result, based on characteristics of individual types of frameworks, the intermediate Csa4Smmes {RSA} framework is regarded as a conceptual framework.

#### 4.4.2 Constructing the intermediate Csa4Smmes {RSA} framework

The intermediate Csa4Smmes {RSA} framework was constructed by using the following building blocks:

- Four high-level stages of the National Institute of Standards and Technology (NIST) framework (Dlamini et al., 2011)
  - Designing an awareness programme
  - Developing awareness material
  - Implementing an awareness programme
  - Post-implementation of the programme
- Plan-Do-Check-Act (PDCA) cycle (ISO/IEC 27000, 2009)
- Process of planning, designing, implementation and evaluation (PDIE) (Dlamini et al., 2011)
- Five layers of the cyber security awareness and education framework (Kortjan & Von Solms, 2014)
  - Strategic layer
  - Tactical layer
  - Preparation layer
  - Delivery layer
  - Monitoring layer
- Ten components of the cyber security awareness framework as discussed in Chapter 3 (Figure 3-4)

These building blocks are discussed firstly to provide context regarding individual building blocks so that the framework can be understood and represented as a summary.

#### 4.4.3 Four high-level stages of the NIST framework

This sub-section provides a discussion on the implementation of the four high-level stages of the National Institute of Standards and Technology (NIST) framework (Labuschagne et al., 2011a). These stages provide guidance to develop cyber security awareness programmes. Therefore, these stages were incorporated into the intermediate Csa4Smme {RSA} framework to provide guidelines for SMMEs to follow while setting up their internal awareness programmes. The high-level stages of the NIST framework include the following:

- *Designing an awareness programme:* It is mandatory to carry out a needs assessment when designing a cyber security awareness programme. This assessment provides feedback concerning current cyber security matters within the organisation. This feedback contributes to shaping the strategy and design of a cyber security awareness programme.
- *Developing awareness materials:* When developing awareness material, it is mandatory to critically address issues regarding awareness topics and necessary sources. However, developing awareness material is dependent on needs assessments. This assessment helps with identifying awareness topics that need to be addressed.
- *Implementing awareness programme:* To implement the awareness programme, it is mandatory to select techniques to deliver awareness messages. The selection of a technique is reliant on accessible resources and the complexity of the message. This level assists in selecting techniques for delivering awareness material.
- *Post-implementation of the programme:* This level assists in evaluating the implemented cyber security awareness programme for monitoring compliance and usefulness. This level ensures that the awareness programme continues to be applicable and compliant with set objectives.

#### 4.4.4 Five layers of the cyber security awareness and education framework

The common elements of cyber security awareness and high-level stages of NIST were discussed previously. This intermediate Csa4Smmes {RSA} framework adopted the structure developed by Kortjan and Von Solms (2014) which is divided into five layers, namely the strategic layer, tactical layer, preparation layer, delivery layer and monitoring layer, and a major component called “Resources” as depicted in Figure 4-3.

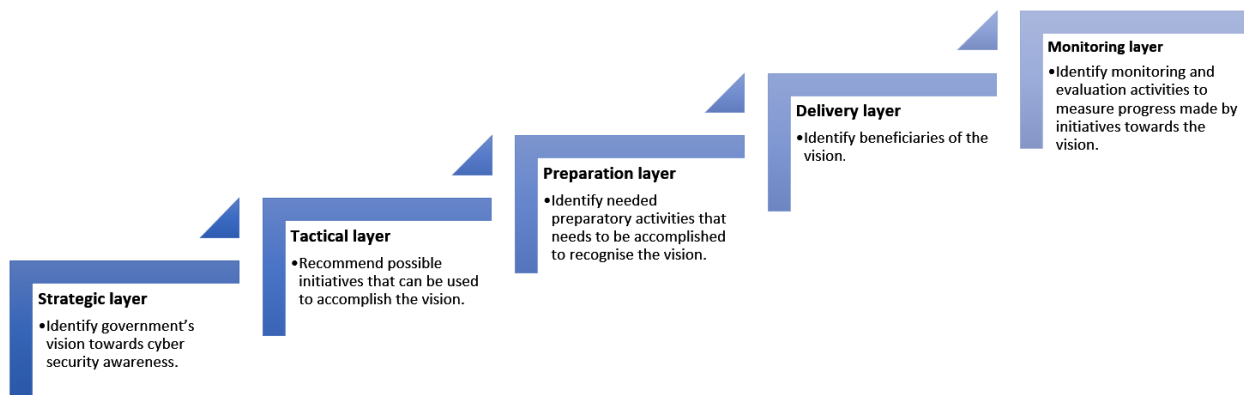


Figure 4-3: Five layers of the intermediate Csa4Smmes {RSA} framework (Kortjan & Von Solms, 2014)

The strategic layer reflects on the government's general vision regarding cyber security awareness. The tactical layer suggests activities that need to be applied to drive cyber security awareness. The preparation layer helps in preparing the content for identified activities. The delivery layer identifies the beneficiaries of the vision. The monitoring layer monitors and evaluates identified activities.

These five layers are aligned with the Plan-Do-Check-Act (PDCA) cycle and the continuous process of planning, designing, implementation and evaluation (PDIE) which will be discussed in the next sub-section (Dlamini et al., 2011). The intermediate Csa4Smmes {RSA} framework incorporated the PDCA cycle and the continuous process of PDIE together. In addition, required resources for these five layers will be discussed.

The intermediate Csa4Smmes {RSA} framework does not replace existing models and frameworks but aims to provide a tailored cyber security awareness framework that is









relevant and suitable for SMMEs, particularly in developing countries – in the context of the study, South Africa. The intermediate Csa4Smmes {RSA} framework was divided into layers as depicted in Figure 4-3.

These layers will be discussed based on models and frameworks that have been adopted in Chapter 3, Table 3-5. In addition, knowledge from the literature review will also be considered. However, the construction of the intermediate Csa4Smmes {RSA} framework was based on models and frameworks which are represented using symbols as shown in Table 4-1.

The following key symbols have been used to emphasise contribution by previously identified models and frameworks that are relevant to the study as shown in Table 4-1:

**Table 4-1: Key symbols for relevant models and frameworks used to identify components of the intermediate Csa4Smmes {RSA} framework**

<b>Symbol</b>	<b>Models and frameworks adopted</b>
	A conceptual framework for cyber security awareness and education in SA (Kortjan & Von Solms, 2014).
	Framework for an African policy for creating cyber security awareness (Dlamini et al., 2011).
	Developing cyber security education and awareness programmes for small and medium-sized enterprises (SMEs) (Bada & Nurse, 2019).
	A framework to integrate ICT security awareness into the South African schooling system (Walaza et al., 2014).
	Ignorance of awareness for an information security awareness process (Gundu & Flowerday, 2013a).
	An information security retrieval and awareness model for industry (Kritzinger, 2006).

Symbol	Models and frameworks adopted
★	This symbol represents a contribution from this research study – Chapter 3: Ten components of cyber security awareness framework.

These keys were used when constructing the intermediate Csa4Smmes {RSA} framework based on the five layers as shown in Figure 4-3. However, the concepts of the PDCA cycle, PDIE and required resources will be discussed first because these five layers are aligned with both the PDCA cycle and PDIE. In addition, required resources for each layer must be identified. Therefore, the PDCA cycle and PDIE will be discussed next, then the required resources, followed by a discussion of each layer.

**4.4.4.1 Plan-Do-Check-Act (PDCA) cycle and continuous cycle of planning, designing, implementation and evaluation (PDIE)**

In this study, the continuous and cycling process of the PDIE and PDCA cycles were integrated together as shown Figure 4-4. This integration was used as a component in the intermediate Csa4Smmes {RSA} framework.



Figure 4-4: PDCA and PDCA integration in the intermediate Csa4Smmes {RSA} framework for SMMEs

**4.4.4.1.a Plan-Do-Check-Act (PDCA) cycle**

These identified layers of the intermediate Csa4Smmes {RSA} framework are continuous and cyclical, meaning they are aligned with the PDCA cycle which is a method that repeats planning, doing, checking and acting phases for continuous improvement (Kortjan & Von Solms, 2014) as shown in Figure 4-5.

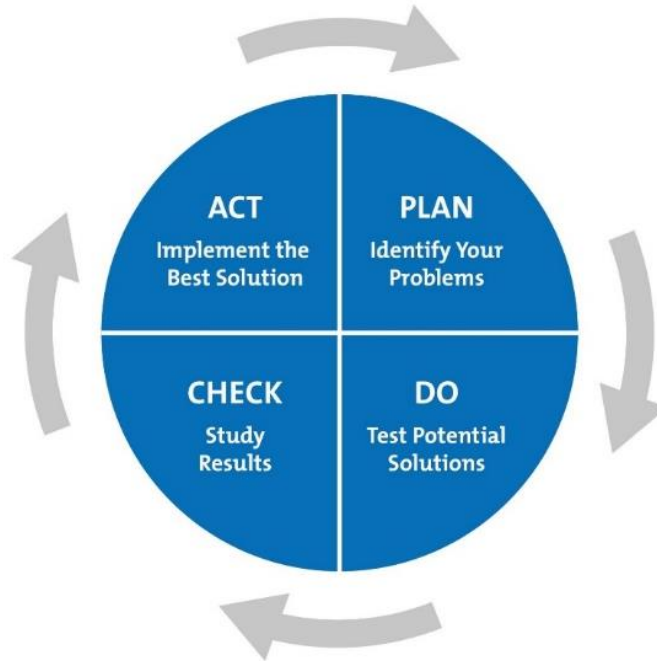


Figure 4-5: PDCA cycle (ISO/IEC 27000, 2009)

The ISO/IEC 27000 implies that the PDCA cycle indicates the following (ISO/IEC 27000, 2009):

- *Plan*: This stage is for identifying and analysing the problem or opportunity to provide particular outcomes. This planning stage is covered in the first (strategic) and second (tactical) layers respectively.
- *Do*: This stage is for implementing the outlined plan and measuring the results. The stage is covered in the third (preparation) and fourth (delivery) layers of the intermediate Csa4Smme {RSA} framework respectively.
- *Check*: This stage is for monitoring and measuring progress against particular requirements. The phase is covered in the fifth (monitoring) layer of the intermediate Csa4Smme {RSA} framework.
- *Act*: This stage is for studying the results and acting according to the triggered responses obtained from the monitoring layer. In this stage, a solution is

implemented.

#### 4.4.4.1.b Process of planning, designing, implementation and evaluation (PDIE)

In addition, the continuous and cycling process of the PDIE and PDCA cycles follows the same procedure; therefore, the intermediate Csa4Smmes {RSA} framework will be in line with the process of PDIE (Dlamini et al., 2011).

- The planning process is covered in the strategic and tactical layers.
- The design process is covered in the preparation layer.
- The implementation is covered in the delivery layer.
- The evaluation is covered in the monitoring layer.

#### 4.4.4.2 Resources

The intermediate Csa4Smmes {RSA} framework integrated an inclusion of resource component as shown in Figure 4-6.

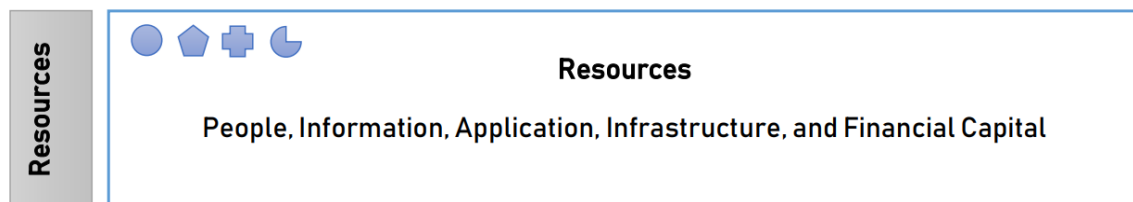


Figure 4-6: Resource components required for the intermediate Csa4Smmes {RSA} framework for SMMEs

Certain resources are to be identified to address all components of the intermediate Csa4Smmes {RSA} framework as identified in each layer. Resources should be in place to support and ensure the successful implementation of each layer (Kritzinger, 2006). Moreover, to achieve the objectives of cyber security awareness, it is recommended that resources be taken into consideration and made available in the intermediate Csa4Smmes {RSA} framework (Kortjan & Von Solms, 2014). This framework should

accomplish and support the vision as stated in the NCPF by helping SMMEs to adhere to their organisational cyber security policy.

The resources component integrates the following component of a cyber security awareness framework as identified in Chapter 3 (Figure 3-4):

- Design an awareness and training strategy.

According to the framework developed by Kortjan and Von Solms (2014), five types of required resources for each layer of the intermediate Csa4Smme {RSA} framework are identified in Figure 4-6. The five types of resources are as follows:

1. People – involvement by individuals to perform certain functions.
2. Information – the information required to execute certain functions.
3. Applications – required computer applications such as software programs.
4. Infrastructure – the required hardware including computing devices.
5. Financial capital – the financial resources that will be required.

The intermediate Csa4Smme {RSA} framework accommodates South African SMMEs and therefore, resources for the intermediate Csa4Smme {RSA} framework will marginally differ from the one developed by Kortjan and Von Solms (2014) which was specifically developed for South African internet users. However, most of the resources within each layer will remain the same. For that reason, the relevant resources that are required per layer of the intermediate Csa4Smme {RSA} framework are to be discussed under each layer.

#### **4.4.4.3 First layer: Strategic layer**

The strategic layer reflects on government's general vision regarding cyber security awareness. As stated in Chapter 1, the South African government primarily aims to promote cyber security in the private sector to establish a support structure that promotes and builds capacity in cyber security (Department of Justice and Constitutional Development, 2017). The general South African vision is to build a cyber security culture

and promote cyber security awareness for South African citizens. In addition, the South African government aims to create an environment where organisations can share responsibilities and contribute to investigating and reporting cybercrimes within the country. Therefore, it is advisable for organisations to have their own in-house cyber security policies.

The strategic layer is aligned with three components, namely the organisational cyber security policy [based on the National Cyber Security Policy Framework (NCPF) and cyber security legislations, procedures, laws and standards], the responsible unit and the strategic plan.

The strategic layer shown in Figure 4-7 integrates the following components of a cyber security awareness framework as identified in Chapter 3 (Figure 3-4):

- Cyber security policy, covered in the strategic layer in the “National Cyber Security Policy Framework (NCPF)” and “Organisational cyber security policy, procedures and standards” (4.4.4.3.a and 4.4.4.3.b respectively in Figure 4-7).
- Establish a security policy, covered in the strategic layer in “Organisational cyber security policy, procedures and standards” (4.4.4.3.c in Figure 4-7).
- Appoint a dedicated team, covered in the strategic layer in “Responsible units” (4.4.4.3.d in Figure 4-7).
- Clearly articulate goals and objectives, covered in the strategic layer in “Strategic plan” (4.4.4.3.e in Figure 4-7).

The strategic layer of the intermediate Csa4Smmes {RSA} framework is presented in Figure 4-7.

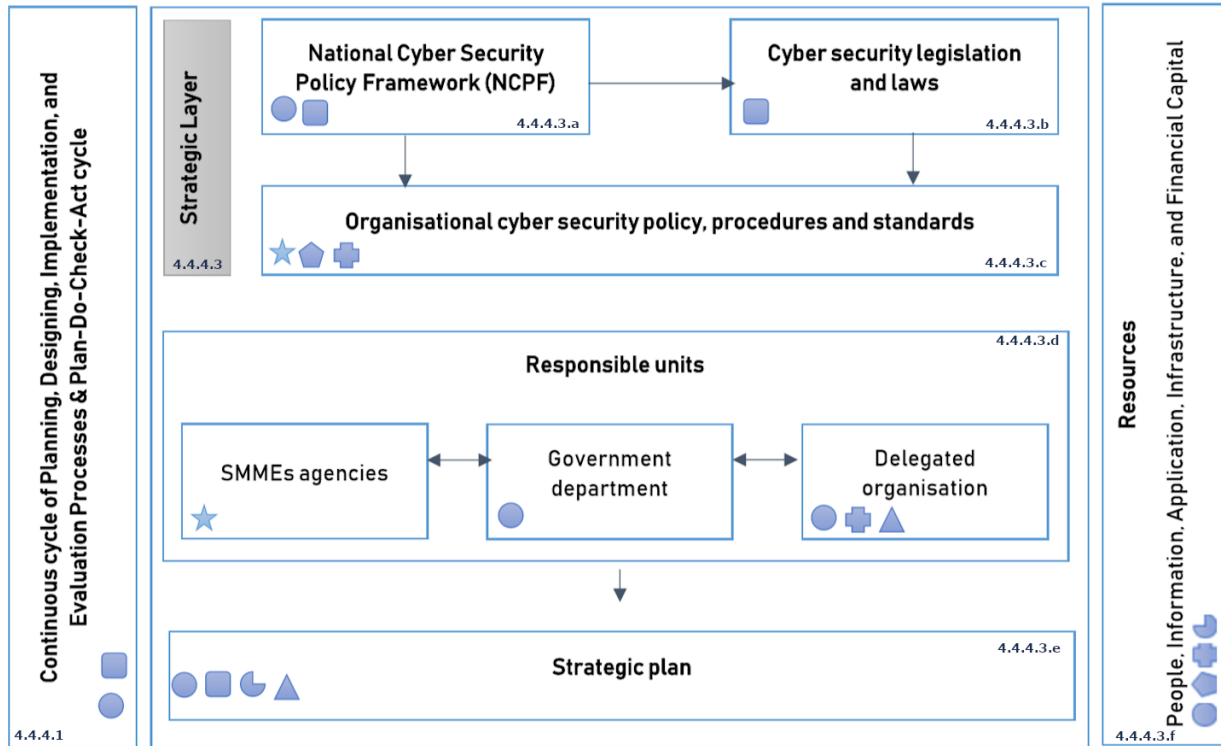


Figure 4-7: The strategic layer of the intermediate Csa4Smms {RSA} framework.

Table 4-2 below explains the different concepts in Figure 4-7 in table format. This table illustrates the responsible parties and corresponding roles and relationships. It consists of the “Component” column, “Parent (sub) component” column, “Child (sub sub) component” column, “Responsible party” column, “Role” column and “Relationship (of components towards each other)” column.

Table 4-2: The relationship between the responsible party and corresponding role in the strategic layer of the intermediate Csa4Smms {RSA} framework

Component	Parent component	Child component	Responsible party	Role	Relationship
National Cyber Security Policy Framework (NCPF) (4.4.4.3.a in Figure 4-7)	None	None	Government	To develop and maintain the NCPF.	Some parts of this component will be used to develop an organisational cyber security

Component	Parent component	Child component	Responsible party	Role	Relationship
					policy, and to influence cyber security legislation and laws.
Cyber security legislation and laws (4.4.4.3.b in Figure 4-7)	None	None	Government	The role of government is to develop and maintain cyber security legislation and laws.	Cyber security legislation and laws are aligned with the NCPF.
Organisational cyber security policy, procedures and standards (4.4.4.3.c in Figure 4-7)	None	None	The delegated organisation, SMMEs and SMME agencies.	To collaborate or individually develop cyber security policy, procedures and standards for a particular SMME.	Cyber security policies, procedures and standards are developed based on cyber security legislation, laws and the NCPF.
Responsible units (4.4.4.3.d in Figure 4-7)	SMME agencies	None	SMME agencies	To develop, support, promote and evaluate cyber security awareness in SMMEs.	To collaborate with other responsible units.
	Government department	None	Government	To collaborate with other units to develop, support, promote and evaluate cyber	To collaborate with other responsible units.



Component	Parent component	Child component	Responsible party	Role	Relationship
				security awareness in SMMEs.	
	Delegated organisation	None	Delegated organisation	To develop, support, promote and evaluate cyber security awareness in SMMEs.	To collaborate with other responsible units.
Strategic plan (4.4.4.3.e in Figure 4-7)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To individually or collaboratively develop a cyber security strategic plan for SMMEs.	Developed through collaboration of identified responsible units.
Resources (4.4.4.3.f in Figure 4-7)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To assist in providing the necessary resources.	Resources can be identified based on all components within the identified layer (where applicable).
Continuous cycle (4.4.4.1 in Figure 4-7)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To ensure the process of planning, doing, monitoring, and implementing works effectively.	Aligned with the identified layer (where applicable).

#### *4.4.4.3.a National Cyber Security Policy Framework (NCPF)*

The NCPF aims to secure and protect the national cyber security infrastructure and to assist in describing the main objective of cyber security awareness (Kortjan & Von Solms, 2014). The NCPF has been developed to respond to the increasing number of cyber attacks (Dlamini et al., 2011). Government is responsible for the development and maintenance of the NCPF. Furthermore, the NCPF describes the standards, procedures, methodologies and processes required to deal with cyber threats and attacks in South Africa (Department of Justice and Constitutional Development, 2017).

#### *4.4.4.3.b Cyber security legislation and laws*

The “Cyber security legislation and laws” component is shown in Figure 4-7. The NCPF, together with cyber security legislation and laws, provides a strong foundation for cyber security awareness initiatives, including models and frameworks. These components complement one another and must be considered when formulating cyber security awareness goals and objectives (Dlamini et al., 2011). Government is responsible to develop and maintain cyber security legislation and laws. These components will be used to formulate an organisational cyber security policy which helps in improving attitudes, behavioural patterns and users’ understanding regarding cyber security (Dlamini et al., 2011).

#### *4.4.4.3.c Organisational cyber security policy, procedures and standards*

The cyber security policy, procedures and standards comprise requirements concerning how employees should conduct themselves while using computing devices within cyberspace (Pattinson, Butavicius, Parsons, McCormac, & Calic, 2017). These policies and procedures can be developed for an organisation through the collaboration of SMMEs, the delegated organisation, government departments and SMME agencies. The organisational cyber security policy will be used as a guideline for describing the main objective concerning cyber security awareness within the organisation.

As shown in Figure 4-7, the organisational cyber security policy, procedures and standards are formulated based on the NCPF and cyber security legislation and laws.

This policy can also be developed based on cyber security best practices established within the body of knowledge. An organisational cyber security policy will therefore be the primary component of the intermediate Csa4Smms {RSA} framework.

Cyber security awareness starts by checking the existence of a cyber security policy within an organisation and then it confirms if the policy is up to date (Gundu & Flowerday, 2013a). The said policy can be used to reduce the cyber security related risks within SMMEs that are associated with human errors (Walaza et al., 2014). This policy also provides governance concerning the utilisation of cyber security assets, devices and infrastructure (Dlamini et al., 2011).

This organisational cyber security policy is mainly formulated to create a cyberspace that is resilient to cyber attacks and where users are knowledgeable regarding cyber security (Kortjan & Von Solms, 2014). Therefore, the organisational cyber security policy can consist of guidelines that will enable SMMEs to be complaint with condition 7 of the POPI Act.

It is also important for employees to recognise and understand cyber security related policies and practices within the organisation (Makhudu, Mavetera, & Mavetera, 2012). According to Makhudu et al. (2012), organisations handle cyber security differently. Some enforce cyber security policies and others do not enforce security policies as they should, while in other organisations, cyber security policies are non-existent. Makhudu et al. (2012) emphasise that fewer employees in SMMEs understand and recognise internal cyber security policies. Subsequently, to fulfil the vision of the NCPF, employees should be aware of organisational cyber security policies, procedures, standards and practices (Gundu & Flowerday, 2013a).

#### *4.4.4.3.d Responsible units*

As identified in the literature review, a dedicated team should be appointed for a variety of reasons. The responsible units are a component of the strategic layer as illustrated in Figure 4-7. Kortjan and Von Solms (2014) state that responsible units can be handled by creating a new administration, utilising existing government department(s) and appointing

a dedicated private or public organisation. Therefore, the identification and appointment of responsible units (also referred as “dedicated teams”) are mandatory because they are responsible for enforcing the adoption of the intermediate Csa4Smms {RSA} framework. The following responsible units can be used to drive the intermediate Csa4Smms {RSA} framework:

### SMME agencies

Von Solms (2015) recommends that SMME agencies such as the Small Business Development Agency (SEDA) evaluate the current cyber conditions in SMMEs because SEDA is an agency responsible for developing, supporting and promoting SMMEs throughout the country. These SMME agencies can individually collaborate with certain government departments, SMMEs and the delegated organisation to develop, support, promote and evaluate cyber security awareness in SMMEs. This collaboration can assist with the process of initialising, driving and evaluating the intermediate Csa4Smms {RSA} framework.

### Government department

One or multiple government departments can be used to evaluate and monitor cyber security awareness for SMMEs (Kortjan & Von Solms, 2014). The National Cyber Security Hub (NCH) is South Africa’s national computer security incident response team (CSIRT) which is mandated by the NCPF to accommodate the public sector, the private sector and civil society (NCH, n.d.). The Electronic Communications Security CSIRT (ECS-CSIRT) is South Africa’s government CSIRT (ECSCSIRT, n.d.). The National Cyber Security Hub and ECS-CSIRT can assist with initialising, driving and evaluating the intermediate Csa4Smms {RSA} framework. The National Research Foundation, South African Agency for Science and Technology Advancement (NRF | SAASTA) is an agency (state-owned enterprise) for science and technology advancement. The NRF | SAASTA can help in implementing this initiative because this organisation is responsible for raising science and technology awareness across South Africa (SAASTA, n.d.). This organisation is well-established and it has footprints across the country through collaboration with science centres in all nine provinces.

Other government departments, including state-owned enterprises such as the Department of Trade and Industry (Dti), the Department of Small Business Development, the Technology Innovation Agency (TIA), the National Youth Development Agency (NYDA) and the Council for Scientific and Industrial Research (CSIR), can collaborate and interact with SMME agencies and the delegated organisation. This collaboration can assist in developing, supporting, promoting and evaluating cyber security awareness in SMMEs.

#### Delegated organisation

A public or private organisation can be delegated to provide SMMEs with cyber security awareness (Von Solms, 2015). The delegated organisation must formulate methods to measure cyber security awareness within South African SMMEs (Walaza et al., 2014). This delegated organisation can be used to engage with South African SMMEs to build solid relationships (Bada & Nurse, 2019). The delegated organisation can also recruit individuals and other organisations (including SMMEs) to voluntarily provide services that are related to the enhancement of cyber security awareness within South African SMMEs.

In addition, multiple organisations can be delegated (through a train-the-trainer approach) to cover SMMEs across all South African provinces. It is recommended that, after the successful appointment of the dedicated organisation, a comprehensive strategic plan be drafted (Kortjan & Von Solms, 2014). The delegated organisation can collaborate and interact with SMME agencies, SMMEs and government departments to develop, support, promote and evaluate cyber security awareness in SMMEs. This organisation can obtain financial support through government grants and incentives, donations, sponsorships, and other financial support to render free services for SMMEs. Alternatively, the delegated organisation can render service directly to SMMEs in form of a paid subscription.

#### *4.4.4.3.e Strategic plan*

The strategic plan indicates strategies that need to be in place in order to accomplish identified cyber security related goals and objectives set by the responsible unit (Kortjan

& Von Solms, 2014). The plan can be utilised to ensure that the awareness content is well-received and for employers and employees to realise an organisation's cyber security awareness goals and objectives (Bada & Nurse, 2019). This plan articulates the approach to be followed to ensure that SMMEs are knowledgeable regarding cyber security.

The strategic plan can be executed at different levels by different sets of responsible units. For example, this strategic plan can be used to ensure that the intermediate Csa4Smme {RSA} framework is assessed for all possible loopholes (Dlamini et al., 2011). Responsible parties can use the strategic plan to identify and organise cyber security related actions within SMMEs (Kritzinger, 2006). The strategic plan can be developed through the collaboration of SMMEs, the delegated organisation, government departments and SMME agencies as identified in Figure 4-7. However, the study will not cover strategic plans in detail.

#### *4.4.4.3.f Resources for strategic layer*

The strategic layer reflects the inclusive vision of government for cyber security awareness within the community of SMMEs. Certain resources are required to be in place for components within the strategic layer. Involvement by competent people will also be required for the development of the strategic plan, establishment of the responsible units and the development of the organisational cyber security policy, procedures and standards. The identified people will also require access to useful information. Furthermore, financial capital (which will not be covered in detail) will be required to access infrastructure and computer applications that are needed to fulfil the effort.

In conclusion, Table 4-3 is a summary of executive roles for relevant components within the strategic layer. The table consists of names of components and parties indicated by "X" to show the ability to execute a specified component. However, some components can be executed or actioned by an individual party or a collaborative effort from multiple parties. For example, SMMEs can execute certain components independently or through the assistance of other parties.

**Table 4-3: Executive roles of components in the strategic layer of the intermediate Csa4Smmes {RSA} framework**

<b>Component</b>	<b>Government departments</b>	<b>Delegated organisation</b>	<b>SMME agency</b>	<b>SMMEs</b>
NCPF	X			
Cyber security legislation and laws	X			
Organisational cyber security policy, procedures and standards		X	X	X
SMME agencies			X	
Government departments	X			
Delegated organisation	X	X	X	X
Strategic plan	X	X	X	X

The next sub-section provides a discussion regarding the second layer, namely the tactical layer.

#### **4.4.4.4 Second layer: Tactical layer**

The tactical layer begins where the first layer left off. The tactical layer suggests activities that need to be applied to drive cyber security awareness. The tactical layer inherits the following components of a cyber security awareness framework as identified in chapter 3 (Figure 3-4):

- Obtain support in the form of partnerships, in the tactic layer covered in partnerships.
- Develop a strategy for implementation, in the tactic layer covered in sub-

campaigns and programmes.

- Design an awareness and training strategy, in the tactic layer covered in sub-campaigns and programmes.

The tactical layer inherits the first high-level outline of the NIST framework. The first sequential step of the NIST framework states that a needs assessment be conducted when designing an awareness programme (Labuschagne et al., 2011a). This process provides SMMEs with assistance to determine cyber security awareness needs within their organisations. The process also helps to identify and understand current cyber security issues that can be used for shaping the strategic plan. It is important to obtain support from management in order for a cyber security awareness programme to be successful (Holdsworth & Apeh, 2017).

The main goal of cyber security awareness is to reduce cyber attacks that are caused by errors due to human factors. Cyber security awareness aims to enhance users' knowledge concerning their responsibility and penalties associated with their cyber security related actions (Al Awawdeh & Tubaishat, 2014). Therefore, the role of cyber security awareness is to contribute to supporting the NCPF objective for creating a cyber security culture within the country.

The tactical layer also suggests activities in the form of campaigns that enable South African SMMEs to understand the cyber security awareness goals identified in the first layer. The proposed name for a cyber security awareness campaign that accommodates SMMEs is *elaTlhoko* as shown in Figure 4-8. *elaTlhoko* is a South African word meaning "be careful, wise up or watch out" in Setswana. This figure presents the tactical layer of the intermediate Csa4Smme {RSA} framework.



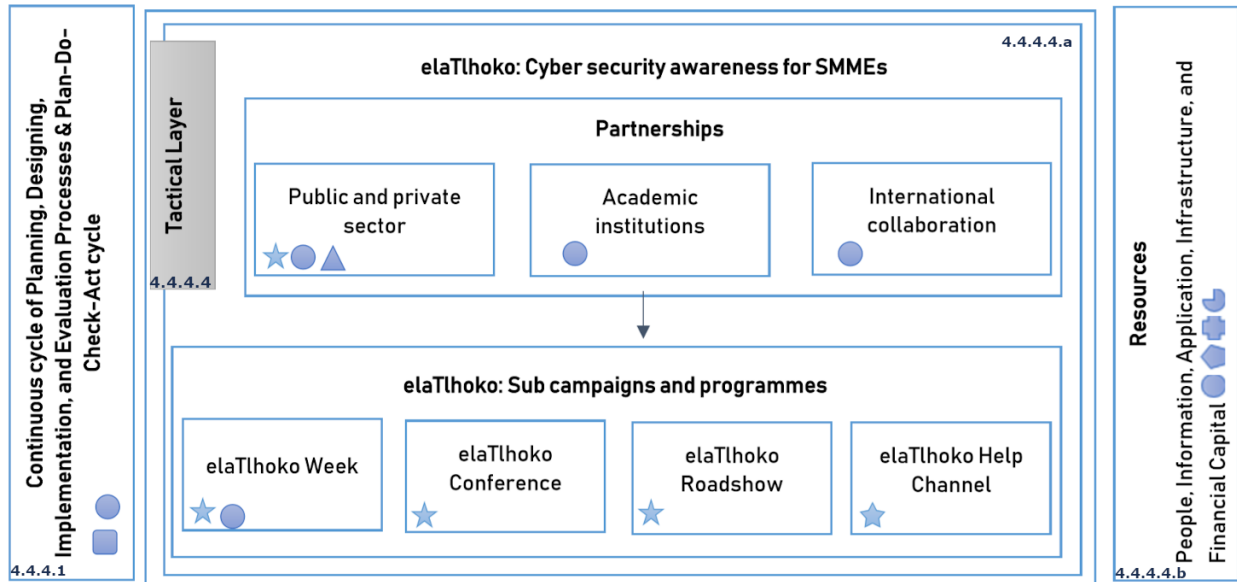


Figure 4-8: The tactical layer of the intermediate Csa4Smmes (RSA) framework

Table 4-4 explains the different concepts in Figure 4-8 in table format. This table illustrates the responsible party and corresponding role and relationship. It consists of the “Component” column, “Parent component” column, “Child component” column, “Responsible party” column, “Role” column and “Relationship” (of components to one another) column in alignment with Figure 4-8.

Table 4-4: The relationship between the responsible party and corresponding role in the tactical layer of the intermediate Csa4Smmes (RSA) framework

Component	Parent component	Child component	Responsible party	Role	Relationship
<i>elaTlhoko</i> : Cyber security awareness for SMMEs (4.4.4.4.a in Figure 4-8)	Partnerships	Public or private sector	Government, delegated public or private organisation in partnership with SMMEs and SMME agencies.	To provide assistance in coordinating certain sections of the <i>elaTlhoko</i> campaign’s action plan.	Collaborating with other partners for a common goal.

Component	Parent component	Child component	Responsible party	Role	Relationship
		Academic institutions	Academic institutions	To assist with distributing cyber security awareness for SMMEs through community engagement and training initiatives (including short courses).	Collaborating with other partners for a common goal.
		International collaboration	Government, the delegated organisation, SMMEs and SMME agencies.	To collaborate and adopt effective initiatives from other countries.	Collaborating with other partners for a common goal.
	<i>elaTlhoko</i> : Sub-campaigns and programmes	<i>elaTlhoko</i> Week	Government, the delegated organisation, SMMEs and SMME agencies.	To initiate and maintain <i>elaTlhoko</i> Week in order to ensure employees, employers and top management in SMMEs are aware of cyber security.	Developed through collaboration of identified partnerships.
		<i>elaTlhoko</i> Conference	Government, the delegated organisation, SMMEs and SMME agencies.	To initiate, maintain and present <i>elaTlhoko</i> Conference through multiple partnerships.	Developed through collaboration of identified partnerships.
		<i>elaTlhoko</i> Roadshow	Government, the delegated organisation, SMMEs and SMME agencies.	To initiate, maintain and present <i>elaTlhoko</i> Roadshow for SMMEs.	Developed through collaboration of identified partnerships.

Component	Parent component	Child component	Responsible party	Role	Relationship
		<i>elaTlhoko</i> Help Channel	Government, the delegated organisation and SMME agencies.	To Initiate, maintain and provide an interactive platform for SMMEs and other partners to communicate with one another.	Developed through collaboration of identified partnerships.
Resources (4.4.4.4.b in Figure 4-8)			Government, the delegated organisation, SMMEs and SMME agencies.	To assist in providing the necessary resources.	Resources can be identified based on all components within the identified layer (where applicable).
Continuous cycle (4.4.4.1 in Figure 4-8)			Government, the delegated organisation, SMMEs and SMME agencies.	To ensure the processes of planning, doing, monitoring and implementing work effectively.	Aligned with the identified layer (where applicable).

#### 4.4.4.4.a *elaTlhoko*: Cyber security awareness for SMMEs

The word *elaTlhoko* warns SMMEs to be cautious about cyber security issues within their organisations. Therefore, it is important for SMMEs to access cyber security awareness campaigns. The establishment of such campaigns requires a collaborative effort from government, the delegated organisation, SMMEs and SMME agencies to reduce successful cyber attacks associated with human errors. This particular campaign consists of identified partnerships which provide assistance within the *elaTlhoko* campaign and its sub-campaigns. Furthermore, a collaborative effort from multiple partners is required to establish cyber security awareness campaigns for South African SMMEs.

## Partnerships

Cyber security policies should include the aspect of public-private partnerships (Von Solms, 2015). For that reason, cyber security awareness campaigns should establish partnerships in order to enable SMMEs and government to collaborate in improving cyber security awareness levels within the country. These partnerships will be established with both the public and private sectors, academic institutions as well as international collaborators (Kortjan & Von Solms, 2014). These partnerships can provide assistance with the *elaTlhoko* sub-campaigns in terms of rolling them out to SMMEs across South Africa.

### *Public and private sector*

Partnerships with public and private organisations should be established because these organisations can assist in coordinating certain sections of the *elaTlhoko* campaign's action plan (Kortjan & Von Solms, 2014). The partnership provides support for raising cyber security awareness for South African SMMEs. In addition, a variety of science centres from multiple locations can be utilised to help with raising cyber security awareness. The involvement of government, SMME agencies and local industrial organisations will help SMMEs by providing guidelines which can be used as a foundation for organisational cyber security (Bada & Nurse, 2019).

### *Academic institutions*

Partnerships with academic institutions, including SMMEs and public and private organisations within the education field, should be established to help with distributing cyber security awareness for SMMEs across South Africa (Kortjan & Von Solms, 2014). These partnerships can also assist with human capacity which is required to effectively distribute cyber security awareness content to SMMEs. These academic institutions can help in formulating a cyber security awareness curriculum, short courses and training for South African SMMEs. These academic institutions could also assist with developing and improving the acceptable body of knowledge regarding cyber security awareness for South African SMMEs.

### *International collaboration*

International collaboration with developing and developed countries should be established to partner, collaborate and adopt effective initiatives from other countries. For example, global projects such as the Cyber Resilience for Development (Cyber4Dev) initiative can be utilised because the Cyber4Dev is a global project by European Union which aims to promote cyber security to protect public and private organisations worldwide (Cyber Resilience for Development, n.d.). The approach can be used to increase cyber security awareness within South African SMMEs. The collaboration helps with aligning the intermediate Csa4Smms {RSA} framework with other similar initiatives from other countries (Kortjan & Von Solms, 2014).

The identified collaboration events will create an environment where SMMEs, government departments, community leaders, municipalities, academic researchers and science centres from other countries can help with enhancing the level of cyber security awareness within SMMEs, ultimately contributing to the whole country's cyber security awareness (Dlamini et al., 2011). The collaboration will also help in identifying and addressing special needs for South African SMMEs. It is also important to obtain support from different parties to promote and enforce cyber security governance within South African SMMEs (Kritzinger, 2006).

### *elaTlhoko: Sub-campaigns and programmes*

The intermediate Csa4Smms {RSA} framework suggests that cyber security awareness campaigns be developed to help SMMEs reduce successful cyber attacks associated with human errors. These campaigns will help fulfil the objective of the NCPF and help SMMEs to implement cyber security related acts. In addition, these campaigns will help individuals within SMMEs to comply with organisational cyber security policy.

Cyber security awareness for SMMEs could be delivered in a variety of ways. The intermediate Csa4Smms {RSA} framework suggests that the *elaTlhoko* campaign be divided into sub-campaigns and programmes to accommodate all individuals within SMMEs. These campaigns should include the South African context and their output

should be tailored to the cyber security needs of SMMEs. The sub-campaigns can be developed through collaboration between government, the delegated organisation, SMMEs and SMME agencies. Therefore, the *elaTlhoko* campaign consists of the following sub-campaigns and programmes:

#### *elaTlhoko* Week

The *elaTlhoko* Week is an annual event that is meant for employees, employers and other people in management positions. The *elaTlhoko* Week focuses on reminding top managers in SMMEs that cyber security is a shared responsibility and serves as an opportunity to spread awareness concerning current cyber security disputes.

#### *elaTlhoko* Conference

The *elaTlhoko* Conference is an annual event intended for establishing collaboration between academics, government departments, the delegated organisation, the private and public sectors and SMMEs (employees and employers). The collaboration creates an environment where various stakeholders can share knowledge, experiences, lessons learnt and initiatives associated with cyber security awareness.

This collaboration enables SMMEs to account for and report on cyber security related challenges they encounter annually because knowledge sharing plays a crucial role in ensuring that acceptable procedures are implemented against cyber crimes (Department of Justice and Constitutional Development, 2017). The conference can also nurture collaboration to improve knowledge sharing and modernise the *elaTlhoko* campaign.

#### *elaTlhoko* Roadshow

The *elaTlhoko* Roadshow aims to provide a collaboration platform between SMMEs, their clients, shareholders, suppliers and customers. This roadshow serves to provide support for SMMEs so as to organise and conduct their own cyber security awareness programmes for both internal and external personnel, including employers, employees and other shareholders.

The *elaTlhoko* Roadshow also aims to provide sufficient support related to cyber security awareness for SMMEs across the country through a train-the-trainer approach. This sub-campaign provides a platform for government departments, the delegated organisation, SMMEs, SMME agencies, public and private companies, academic researchers and science centres to participate voluntarily in spreading cyber security awareness in SMMEs across the country. The campaign can provide incentives such as public recognition, recommendations, promotions, badges, corporate and gift cards and certificates for hardworking SMMEs that embrace cyber security awareness for both their internal and external personnel.

#### *elaTlhoko* Help Channel

The *elaTlhoko* Help Channel provides an interactive platform for SMMEs to communicate with one another. The Help Channel enables government departments, the delegated organisation, SMME agencies, academics, public and private companies, science centres, individuals and SMMEs to remotely share knowledge regarding cyber security awareness. This platform can be driven through the internet, while interested parties collaborate and interact with one another through the social networking environment. This campaign oversees the *elaTlhoko* campaign and is intended to handle all communications regarding *elaTlhoko* campaigns. The interactive platform can be used as a small business CSIRT that provides a 24/7 cyber security related service in order to enhance cyber security awareness for employees and employers within SMMEs (Von Solms, 2015).

The *elaTlhoko* cyber security awareness campaign and its sub-campaigns are the main features of the tactical layer. These campaigns are implemented to drive cyber security awareness for SMMEs across the country. However, the awareness topic(s), awareness scope, awareness content, delivery methods and tools should be considered when providing a tailored cyber security awareness campaign.

#### 4.4.4.4.b Resources for the tactical layer

The tactical layer provides a guideline that suggests initiatives to enhance cyber security awareness in SMMEs. Firstly, a dedicated team will be tasked to initiate the *elaTlhoko* campaign, including its sub-campaigns and programmes. Secondly, information is required to provide appropriate guidelines to create and launch a cyber security awareness campaign. Lastly, financial support will be required to launch the *elaTlhoko* initiative.

In conclusion, Table 4-5 is a summary of the executive roles for relevant components within the tactical layer. The table consists of the names of the components and parties indicated by “X” to show the ability to execute a specified component. However, some components can be executed or actioned by an individual party or a collaborative effort from multiple parties.

**Table 4-5: Executive roles for components in the tactical layer of the intermediate Csa4Smmes (RSA) framework**

<b>Component</b>	<b>Government departments</b>	<b>Delegated organisation</b>	<b>SMME agency</b>	<b>SMMEs</b>
Public or private sector	X	X	X	X
Academic institutions		X		X
International collaboration	X	X	X	X
<i>elaTlhoko</i> Week	X	X	X	X
<i>elaTlhoko</i> Conference	X	X	X	X
<i>elaTlhoko</i> Roadshow	X	X	X	X
<i>elaTlhoko</i> Help Channel	X	X	X	X



The next sub-section introduces the next layer that takes over from the tactical layer.

#### **4.4.4.5 Third layer: Preparation layer**

The preparation layer helps with preparing the content for the *elaTihoko* campaign as documented in the tactical layer. Cyber security awareness efforts are intended to change behaviour or strengthen good cyber security practices (Hassanzadeh et al., 2013). The purpose of awareness presentations is to use attractive techniques to focus attention on cyber security to assist users in identifying cyber security concerns and react accordingly.

The preparation layer illustrated in Figure 4-9 inherits the following components of a cyber security awareness framework identified in Chapter 3 (Figure 3-4):

- Awareness scope, in the preparation layer covered in “Awareness scope” (4.4.4.5.a in Figure 4-9).
- Identify current training needs, in the preparation layer covered in “Awareness topics” and “Awareness content” (4.4.4.5.b and 4.4.4.5.c respectively in Figure 4-9).
- Define topics to cover and their delivery methods, in the preparation layer covered in “Awareness topics” and “Delivery method” (4.4.4.5.b and 4.4.4.5.d respectively in Figure 4-9).

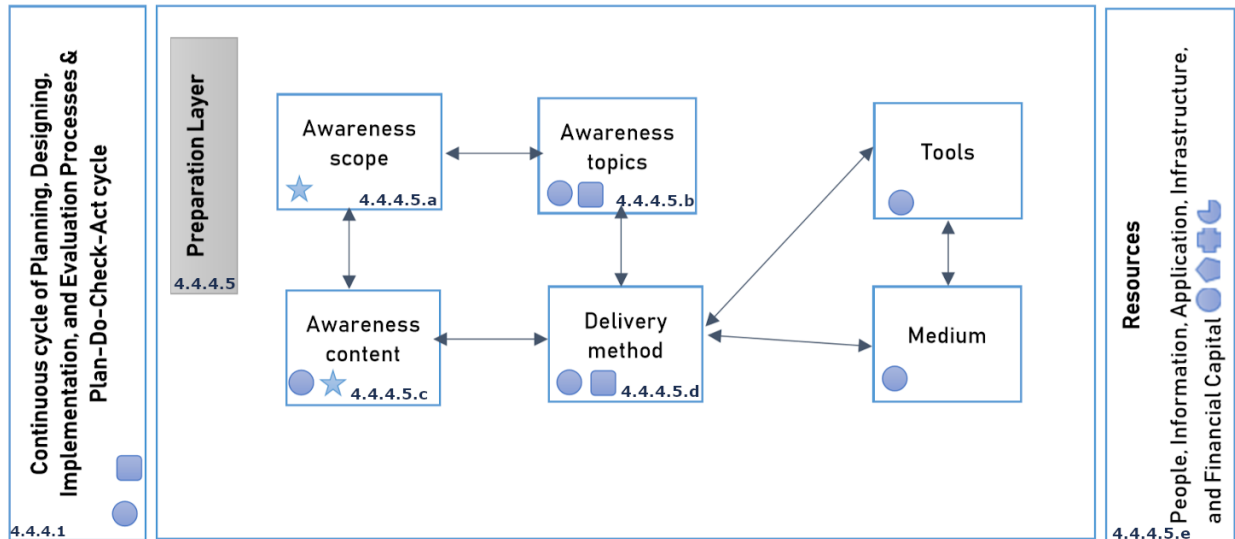


Figure 4-9: The preparation layer of the intermediate Csa4Smms {RSA} framework.

The preparation layer is made up of four components, namely awareness scope, awareness topics, awareness content and delivery methods, including medium and tools. Table 4-6 explains the different concepts in Figure 4-9 in table format. It consists of the “Component” column, “Parent component” column, “Child component” column, “Responsible party” column, “Role” column and “Relationship” (of components towards each other) column in alignment with Figure 4-9. This table illustrates the responsible party and corresponding role and relationship.

Table 4-6: The relationship between the responsible party and corresponding role in the preparation layer of the intermediate Csa4Smms {RSA} framework

Component	Parent component	Child component	Responsible party	Role	Relationship
Awareness scope (4.4.4.5.a in Figure 4-9)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To collaboratively develop a tailored awareness scope aligned to the cyber security vision and mission within a SMME. However, the	Aligned with cyber security awareness content and topics.

Component	Parent component	Child component	Responsible party	Role	Relationship
				scope could be generic to accommodate external parties.	
Awareness topics (4.4.4.5.b in Figure 4-9)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	A collaborative effort to identify cyber security awareness topics for a particular SMME; however, other topics are generic.	Awareness topics are aligned with the selected delivery methods.
Awareness content (4.4.4.5.c in Figure 4-9)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	A collaborative effort to develop and maintain cyber security awareness content for SMMEs.	Awareness content is aligned with the selected delivery methods.
Delivery methods (4.4.4.5.d in Figure 4-9)	Tools	None	Government, the delegated organisation, SMMEs and SMME agencies.	To collaboratively identify tools to be used when conducting cyber security awareness in SMMEs	The selection of tools are aligned with cyber security awareness topic, content and medium.
	Medium	None	Government, the delegated organisation, SMMEs and SMME agencies.	A collaborative effort to identify communication medium to be used when delivering cyber security	The selection of the medium is aligned with target audiences and awareness topics and content.

Component	Parent component	Child component	Responsible party	Role	Relationship
				awareness in a particular SMME.	
Resources (4.4.4.5.e in Figure 4-9)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To assist in providing necessary resources.	Resources can be identified based on all components within the identified layer (where applicable).
Continuous cycle (4.4.4.1 in Figure 4-9)	None	None	Government, the delegated organisation, SMMEs and SMME agencies.	To ensure the process of planning, doing, monitoring and implementing works effectively.	Aligned with the identified layer (where applicable).

#### 4.4.4.5.a Awareness scope

Awareness scope helps in simplifying awareness content so that it becomes easy for the target audience to understand benefits to be gained or risks to be mitigated through a cyber security awareness programme (Al Awawdeh & Tubaishat, 2014). The delivery of cyber security awareness content should be attractive, applicable and continuous. The content comprises a variety of relevant topics as per the target audience (Ki-Aries & Faily, 2017). The scope of awareness should be addressed because it plays an important role in the success of implementing any cyber security awareness programme (Al Awawdeh & Tubaishat, 2014).

A cyber security awareness scope must be aligned with the cyber security vision and mission of SMMEs because it is intended to make all users within SMMEs conscious about goals and objectives of the awareness programme. In addition, collaboration between government, the delegated organisation, SMMEs and SMME agencies assists

with the development of a tailored awareness scope which is aligned with the cyber security vision and mission of SMMEs.

Cyber security awareness scope, topics, content and delivery methods will vary to accommodate different groups of target audiences. However, the awareness scope for SMMEs could be generic to accommodate stakeholders. Generic cyber security awareness scope, topics, content and delivery methods can be developed through collaboration and made available for SMMEs to customise based on their requirements.

#### *4.4.4.5.b Awareness topics*

Employees and employers within SMMEs should only learn about cyber security awareness topics that are relevant and customised as per their job responsibilities. However, other cyber awareness topics such as password management, information handling, social networks and social engineering are generic. It is important for a cyber security awareness programme to provide tailored topics and delivery methods that are best suited for individuals within organisations (Kortjan & Von Solms, 2014).

The preparation layer inherits the second and third high-level outline of the NIST framework stating that needs assessment can be conducted in order to identify relevant topics and delivery methods for different target audiences (Dlamini et al., 2011). Therefore, it is advisable to use multiple forms of media techniques.

As identified in Chapter 3, cyber security awareness topics have been identified through a systematic literature study. The intermediate Csa4Smmes {RSA} framework suggests that awareness topics be tailored in order to deliver (cyber security related) awareness that is suitable for SMMEs in developing countries, specifically in South Africa (Kortjan & Von Solms, 2014). These awareness topics are determined by collaboration between government, the delegated organisation, SMMEs and SMME agencies.

According to Kritzinger and Smith (2008), job classifications in organisations will vary from one organisation to another. Therefore, it is important to acknowledge not to overburden employees with unnecessary information that is not relevant to their specific job function because it is irrational to expect them to be cognisant of all cyber security issues. The

distribution of customised content and delivery methods should be planned and implemented (Ki-Aries & Faily, 2017). Furthermore, Kortjan and Von Solms (2014) agree that there is a relationship between topic and content. This relationship is guided by awareness materials and content that will be used for certain target audiences.

#### *4.4.4.5.c Awareness content*

Cyber security awareness content should be relevant to enable tailored learning content so that individuals can focus on content related to their job description (Holdsworth & Apeh, 2017). Awareness content should be distributed to the correct identified target audience (Kortjan & Von Solms, 2014; Yunus, Hamid, & Ahmad, 2016) in order to simplify the delivered information and materials. Cyber security awareness content should be developed based on organisational cyber security policy, organisational cyber security needs, international cyber security standards, common cyber security errors made by employees, delivery methods and also targeted audience profiles (Amankwa et al., 2016; Ghazvini & Shukur, 2017). An establishment and maintenance of cyber security awareness content will be determined by a collaborative effort from government, the delegated organisation, SMMEs and SMME agencies.

#### *4.4.4.5.d Delivery methods*

The relationship between content and medium recommends that an appropriate communication medium and tools be selected based on the combination of awareness topics and content (Dlamini et al., 2011; Kortjan & Von Solms, 2014). The preparation layer helps with preparing cyber security awareness campaigns for SMMEs. The collaboration of government, the delegated organisation, SMMEs and SMME agencies will assist in developing delivery methods such as conventional, instructor-led, online, game-based, video-based and simulation-based delivery methods appropriate for SMMEs (Abawajy, 2014). Moreover, generic delivery methods, including tools and medium, will be developed for SMMEs to customise based on their requirements.

## Tools

The *elaTlhoko* initiative provides certain tools which can be utilised to convey the cyber security awareness message for SMMEs (Kortjan & Von Solms, 2014). These tools can be influenced based on different environments within SMMEs. Therefore, it is important to select and define tools when conducting cyber security awareness, and this selection process should be based on the awareness topic, awareness content and medium (Kortjan & Von Solms, 2014). The collaboration of government, the delegated organisation, SMMEs and SMME agencies will provide assistance to identify tools such as organisational newsletters and memos, email messages, posters, screensavers, security labels, games, videos, social media posts and training materials for conducting cyber security awareness for SMMEs.

## Medium

The selection of the communication medium utilised for delivering cyber security awareness should be tailored based on the target audience (Kortjan & Von Solms, 2014). It is important to clearly define awareness topics and content to select an appropriate medium of communication, being paper-based and/or electronic. The collaboration of government, the delegated organisation, SMMEs and SMME agencies will provide assistance to identify appropriate communication mediums for delivering cyber security awareness to SMMEs.

### *4.4.4.5.e Resources for the preparation layer*

The preparation layer helps with the process of preparing content for the *elaTlhoko* initiative. In this layer, competent people should be in place to define topics, content and delivery methods (tools and medium). Relevant information is required to determine which topics to cover for all identifiable target audience groups. This information will be used as a guideline to determine which topics and content to cover and which method of delivery to use.

Computer applications and infrastructure are also needed for establishing the tailored cyber security awareness scope, topics, content and delivery methods for each target audience. Finally, financial capital is required to obtain the necessary resources.

In conclusion, Table 4-7 is a summary of the executive roles for relevant components within the preparation layer. The table consists of names of components and parties indicated by “X” to show the ability to execute a specified component. However, some components can be executed or actioned by an individual party or a collaborative effort from multiple parties.

**Table 4-7: Executive roles for components in the preparation layer of the intermediate Csa4Smms (RSA) framework**

<b>Component</b>	<b>Government departments</b>	<b>Delegated organisation</b>	<b>SMME agency</b>	<b>SMMEs</b>
Awareness scope	X	X	X	X
Awareness topics	X	X	X	X
Awareness content	X	X	X	X
Tools	X	X	X	X
Medium	X	X	X	X

The next layer to be discussed is the delivery layer which helps in identifying the target audience.

**4.4.4.6 Fourth layer: Delivery layer**

The fourth layer helps with the delivery of cyber security awareness as shown in Figure 4-10. The delivery layer defines the target audience as per preparations made in the previous layer. The delivery layer inherits the following components of a cyber security awareness framework identified in Chapter 3 (Figure 3-4):



- Identify target audiences, in the delivery layer covered in “*elaTlhoko*: Target audience and roles” (4.4.4.6.a in Figure 4-10).
- Obtain support in the form of partnerships, in the delivery layer covered in “*elaTlhoko*: Target audience and roles” (4.4.4.6.a in Figure 4-10).

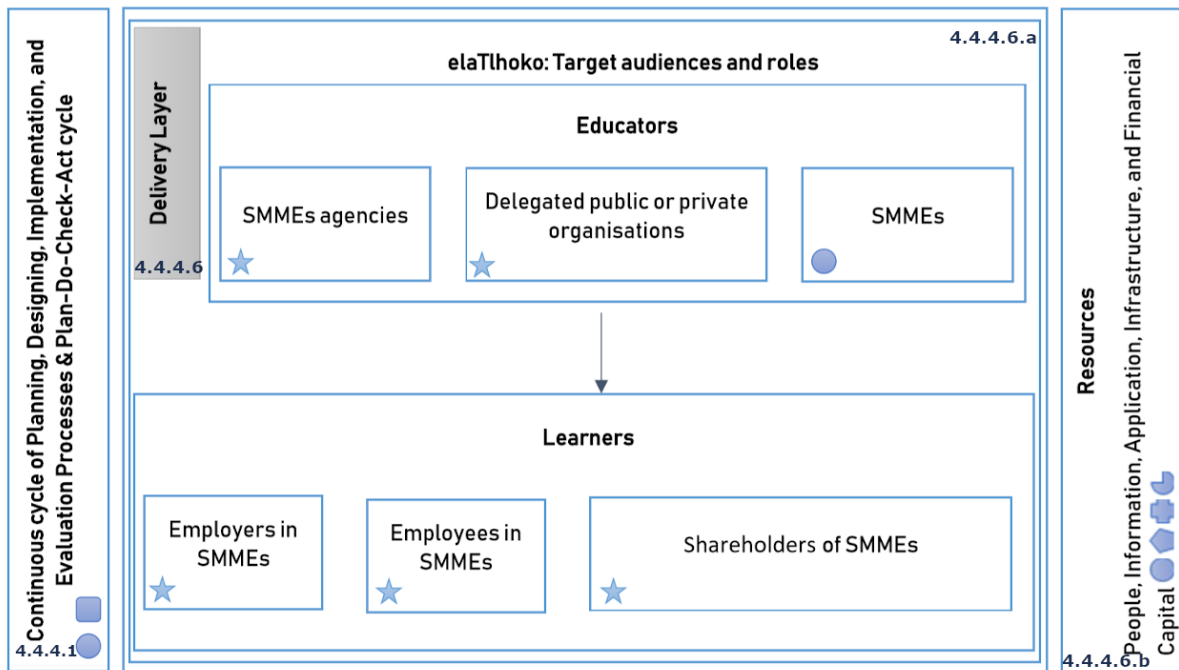


Figure 4-10: The delivery layer of the intermediate Csa4Smms {RSA} framework

Table 4-8 below explains the different concepts in Figure 4-10 in table format. It consists of the “Component” column, “Parent component” column, “Child component” column, “Responsible party” column, “Role” column and “Relationship” (of components towards each other) column in alignment with Figure 4-10. This table illustrates the responsible party and corresponding role and relationship.

Table 4-8: The relationship between the responsible party and corresponding role in the delivery layer of the intermediate Csa4Smms {RSA} framework

Component	Parent sub-component	Child sub-component	Responsible party	Role	Relationship
<i>etla Tlhoko:</i> Target audience and roles (4.4.4.6.a in Figure 4-10)	Educators	SMME agencies	SMME agencies	To provide cyber security awareness for employers, employees and stakeholders within SMMEs.	Provides cyber security awareness for target audience playing a learner's role.
		Delegated public or private organisations	Delegated public or private organisations	To provide cyber security awareness for employers, employees and stakeholders within SMMEs.	Provides cyber security awareness for target audience playing a learner's role.
		SMMEs	SMMEs	To provide cyber security awareness for employers, employees and stakeholders within SMMEs.	Provides cyber security awareness for target audience playing a learner's role.
	Learners	Employers in SMMEs	SMMEs	To receive awareness from SMME agencies, delegated organisations and SMMEs.	Acquires cyber security awareness from educators.
		Employees in SMMEs	SMMEs	To receive awareness from SMME agencies, delegated organisations and SMMEs.	Acquires cyber security awareness from educators.

Component	Parent sub-component	Child sub-component	Responsible party	Role	Relationship
		Stakeholders of SMMEs	SMMEs	To receive awareness from SMMEs agencies, delegated organisations and SMMEs.	Acquires cyber security awareness from educators.
Resources (4.4.4.6.b in Figure 4-10)			Government, the delegated organisation, SMMEs and SMME agencies.	To assist in providing the necessary resources.	Resources can be identified based on all components within the identified layer (where applicable).
Continuous cycle (4.4.4.1 in Figure 4-10)			Government, the delegated organisation, SMMEs and SMME agencies.	To ensure the process of planning, doing, monitoring and implementing works effectively.	Aligned with the identified layer (where applicable).

**4.4.4.6.a etlaTlhoko: Target audience and roles**

The awareness scope must consider both internal and external personnel within SMMEs such as employers, employees, supply chain partners, subcontractors, customers, vendors and other stakeholders who interact with the organisation on a regular basis. The target audiences must be identified, grouped into categories such as top management, IT and security staff or end-users and addressed independently in order to ensure that awareness campaigns are more effective (Al Awawdeh & Tubaishat, 2014). These target audience groups represent all users performing a variety of duties within SMMEs regardless of the operational industry. In this layer, identified target audiences will play different roles, namely those of the educator role and a learner (Kortjan & Von Solms, 2014).

## Educators

Educators are responsible to carefully monitor learners, attend to their questions, comments and inspiration, and provide a variety of opportunities related to their inspiration (Fry, Ketteridge, & Marshallis, 2008). These opportunities are provided for further exploration. Educators are responsible for providing cyber security awareness for target audience playing a learner's role. SMME agencies, the delegated organisation and SMMEs will play the educator role as follows:

### *SMME agencies*

SMME agencies such as the Small Business Development Agency (SEDA) and the Small Enterprise Finance Agency (SOF) Limited (SEFA) can play an educator's role by providing cyber security awareness courses to employers, employees and stakeholders within SMMEs. The SEDA is responsible for developing, empowering and supporting SMMEs while the SEFA is responsible for providing South African SMMEs with simple access to finance in an efficient and sustainable manner. SMME agencies can voluntarily utilise their resources to cover a large number of SMMEs that play a learner's role. The relationship with SMME agencies can be established through an individual effort or collaboration with government departments, the delegated organisation and SMMEs.

### *Delegated public or private organisations*

Delegated public or private organisations such as NRF | SAASTA, science centres, academic institutions and government departments can play the educator's role by providing cyber security awareness to employers, employees and stakeholders within SMMEs. Partnerships with multiple delegated organisations can be established to provide a platform for these delegated organisations to voluntarily provide cyber security awareness to SMMEs who play a learner's role. The relationship with delegated organisations can be established through an individual effort or a collaboration with government departments, SMME agencies and SMMEs.

## *SMMEs*

SMMEs can also play the educator's role through a train-the-trainer approach where knowledgeable SMMEs share skills and knowledge with other SMMEs playing a learner's role and lacks cyber security awareness. These SMMEs will provide cyber security awareness to employers, employees and stakeholders within these SMMEs. Government departments, delegated organisations and SMME agencies can also provide support for SMMEs playing the educator's role.

## Learners

The main roles of learners are to acquire knowledge, continuously study and practise and conduct assessments as prescribed by their educators. Learners are responsible to listen and pay attention during sessions (Fry et al., 2008). They are responsible for their own learning development regarding a particular subject matter. A learner's role will be played by employers, employees and stakeholders in SMMEs.

## *Employers in SMMEs*

Employers within SMMEs can play a learner's role when they receive cyber security awareness information from SMME agencies, delegated organisations and SMMEs playing the educator's role.

## *Employees in SMMEs*

Employees within SMMEs can also play a learner's role when they too receive cyber security awareness information from SMME agencies, delegated organisations and SMMEs playing the educator's role.

## *Stakeholders of SMMEs*

Stakeholders of SMMEs such as customers, clients and partners can also play a learner's role. These stakeholders can receive cyber security awareness information from SMMEs individually or in collaboration with SMME agencies and delegated organisations playing the educator's role.

Cyber security awareness content must be formulated based on the targeted audience (Ghazvini & Shukur, 2017) and balanced and tailored as per the identified target audience because if the message was not easy to understand, novice users would lose interest whereas if an easy message was presented, professional users would be bored.

#### 4.4.4.6.b Resources for delivery layer

The delivery layer helps with the process of identifying target audiences according to preparations made in the previous layer. Within the delivery layer, information is required as an input. This information provides guidelines to oversee how target audiences should play their allocated roles.

In conclusion, Table 4-9 is a summary of the executive roles for the relevant components within the delivery layer. The table consists of the names of components and parties indicated by “X” to show the ability to execute a specified component. However, some components can be executed or actioned by an individual party or a collaborative effort from multiple parties.

**Table 4-9: Executive roles of components in the delivery layer of the intermediate Csa4Smmees {RSA} framework**

<b>Component</b>	<b>Government departments</b>	<b>Delegated organisation</b>	<b>SMME agency</b>	<b>SMMEs</b>
SMME agencies	X	X	X	X
Delegated public or private organisation	X	X	X	X
SMMEs	X	X	X	X
Employers in SMMEs		X	X	X
Employees in SMMEs		X	X	X
Stakeholders of SMMEs		X	X	X

This campaign must be evaluated for efficiency towards achieving its projected goals. Therefore, the next section provides a discussion regarding the fifth layer which is the monitoring layer.

#### 4.4.4.7 Fifth layer: Monitoring layer

The monitoring layer helps with the process of examining progress made by *elaTlhoko* initiatives regarding the organisational and national vision for cyber security awareness. The *elaTlhoko* campaign must be monitored and evaluated for effectiveness as shown in Figure 4-11 which provides a visual presentation of the monitoring layer. This layer, as illustrated on Figure 4-11, inherits the following components of a cyber security awareness framework as identified in Chapter 3 (Figure 3-4):

- Develop evaluation methods, in the monitoring layer covered in the “Evaluation” component (4.4.4.7.a in Figure 4-11).

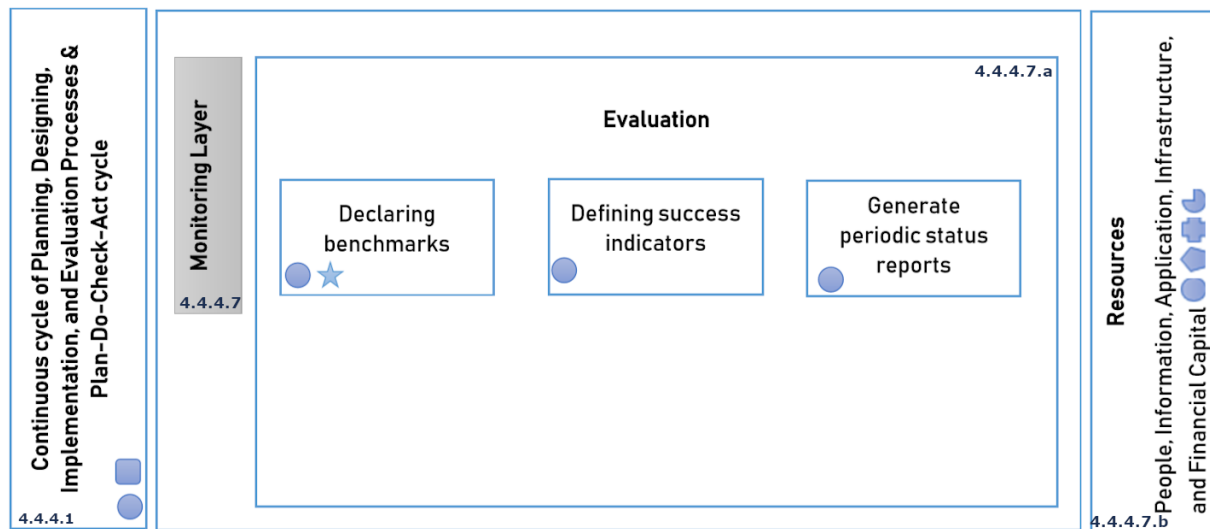


Figure 4-11: The monitoring layer of the intermediate Csa4SmmeS {RSA} framework

Table 4-10 below explains the different concepts in Figure 4-11 in table format. It consists of the “Component” column, “Parent component” column, “Child component” column, “Responsible party” column, “Role” column and “Relationship” (of components towards

each other) column in alignment with Figure 4-11. This table illustrates the responsible party and corresponding role and relationship.

**Table 4-10: The relationship between the responsible party and corresponding role in the monitoring layer of the intermediate Csa4Smmes {RSA} framework**

Component	Parent sub-component	Child sub-component	Responsible party	Role	Relationship
Evaluation (4.4.4.7.a in Figure 4-11)	Declaring benchmarks		Government, the delegated organisation, SMMEs and SMME agencies.	To state and declare benchmarks regarding projected targets and standards.	This process is executed to evaluate the effectiveness of the cyber security awareness campaign and the intermediate Csa4Smmes {RSA} framework.
	Defining success indicators		Government, the delegated organisation, SMMEs and SMME agencies.	To monitor and evaluate the cyber security awareness, campaign and the intermediate Csa4Smmes {RSA} framework.	This process is executed to evaluate the effectiveness of cyber security awareness, campaign and the intermediate Csa4Smmes {RSA} framework.
	Generate periodical status report		Government, the delegated organisation, SMMEs and SMME agencies.	To collaboratively generate periodical status reports to keep track of the progress of the cyber security awareness campaign and the intermediate	This process is executed to evaluate the effectiveness of the cyber security awareness campaign and the intermediate Csa4Smmes {RSA} framework.



Component	Parent sub-component	Child sub-component	Responsible party	Role	Relationship
				Csa4Smmes {RSA} framework.	
Resources (4.4.4.7.b in Figure 4-11)			Government, the delegated organisation, SMMEs and SMME agencies.	To assist in providing the necessary resources.	Resources can be identified based on all components within the identified layer (where applicable).
Continuous cycle (4.4.4.1 in Figure 4-11)			Government, the delegated organisation, SMMEs and SMME agencies.	To ensure the process of planning, doing, monitoring and implementing works effectively.	Aligned with the identified layer (where applicable).

**4.4.4.7.a Evaluation**

The monitoring layer inherits the last component of the cyber security awareness framework as identified in Chapter 3 (Figure 3-4). This layer was inherited to define and develop evaluation methods. The monitoring layer inherits the fourth high-level outline of the NIST framework which is called “Post-implementation of the programme”. It assists in evaluating the effectiveness of the cyber security awareness *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework. Government, the delegated organisation, SMMEs and SMME agencies can assist regarding monitoring and evaluation which can be used to continuously improve the existing awareness campaign (Dlamini et al., 2011). According to Kortjan and Von Solms (2014), these processes can be accomplished by:

Declaring benchmarks

Monitoring and evaluation can be accomplished by stating and declaring benchmarks regarding projected targets and standards (Kortjan & Von Solms, 2014). This process assists with comparing the effectiveness of the cyber security awareness *elaTlhoko*

campaign and the intermediate Csa4Smmes {RSA} framework) between the initial state and the projected targets and standards. This process can be established and managed by government, the delegated organisation, SMMEs and SMME agencies. SMMEs can individually or collectively collaborate with government, the delegated organisation and SMME agencies to formulate benchmarks related to cyber security awareness. However, government, the delegated organisation and SMME agencies can declare benchmarks related to the *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework.

#### Defining success indicators

The process of defining success indicators can be used to monitor and evaluate the cyber security awareness *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework (Kortjan & Von Solms, 2014). These indicators can be used to measure the difference between success and failure of the cyber security awareness *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework. These success indicators can be defined and managed by government, the delegated organisation, SMMEs and SMME agencies. SMMEs can individually or collectively collaborate with government, the delegated organisation and SMME agencies to define the success indicators for their internal cyber security awareness. However, government, the delegated organisation and SMME agencies can define the success indicators related to the *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework.

#### Generating periodical status reports

Generating periodical status reports can be used as a monitoring and evaluation method (Kortjan & Von Solms, 2014). These reports can be used to keep track of the progress made with the cyber security awareness *elaTlhoko* campaign and the intermediate Csa4Smmes {RSA} framework to create visibility and accountability concerning the progress of the intermediate Csa4Smmes {RSA} framework. This process can be established and managed by government, the delegated organisation, SMMEs and SMME agencies. SMMEs can individually or collectively collaborate with government, the delegated organisation and SMME agencies to generate cyber security awareness related periodical status reports. However, government, the delegated organisation and

SMME agencies can generate periodical status reports for the *elaTlhoko* campaign and the intermediate Csa4Smms {RSA} framework.

It is important to ensure that the current awareness level of cyber security is satisfactory. This evaluation helps to identify knowledge gaps regarding cyber security understanding within SMMEs (Gundu & Flowerday, 2013a). Certain mechanisms are required to be utilised by SMMEs to evaluate and monitor cyber security awareness and other activities related to cyber security (Walaza et al., 2014). This phase is important because evaluation helps to indicate if the *elaTlhoko* campaign has a positive or a negative effect on South African SMMEs, while monitoring helps to identify if the *elaTlhoko* campaign and the intermediate Csa4Smms {RSA} framework have been implemented correctly within SMMEs as they are supposed to be (Kritzinger, 2006).

#### *4.4.4.7.b Resources for the monitoring layer*

The monitoring layer helps with inspecting the progress made by the initiative concerning the fulfilment of government’s vision for cyber security awareness. In the monitoring layer, competent people are required to lead the process of defining benchmarks and identifying the required success factors that can be used for examining the initiative. Furthermore, information, computer applications and infrastructure will be required to generate periodical reports to evaluate the initiative. Similarly, adequate financial support should be made available to meet expenditure on additional resources. In conclusion, each layer of the intermediate Csa4Smms {RSA} framework will require one or more resources to ensure that all components of each layer are prepared.

Table 4-11 below is a summary of the executive roles of the relevant components within the monitoring layer. The table consists of the names of the components and parties indicated by “X” to show the ability to execute a specified component. However, some components can be executed or actioned by an individual party or a collaborative effort from multiple parties.

**Table 4-11: Executive roles of components in the monitoring layer of the intermediate Csa4Smms {RSA} framework**

Component	Government departments	Delegated organisation	SMME agency	SMMEs
Declaring benchmarks	X	X	X	X
Defining success indicators	X	X	X	X
Generating periodical status reports	X	X	X	X

This sub-section provided a discussion about the components of the intermediate Csa4Smmes {RSA} framework. Therefore, the next sub-section provides an overview of the intermediate Csa4Smmes {RSA} framework structure.

**4.4.5 The intermediate Csa4Smmes {RSA} framework**

This section provides the intermediate Csa4Smmes {RSA} framework as discussed in the previous section. In this section, all identified components of cyber security awareness framework were assembled to construct the intermediate Csa4Smmes {RSA} framework. Figure 4-12 is the intermediate Csa4Smmes {RSA} framework which will be validated in the next chapter. This framework was constructed by integrating previously discussed layers together, connected through arrows which signify the flow of the intermediate Csa4Smmes {RSA} framework.

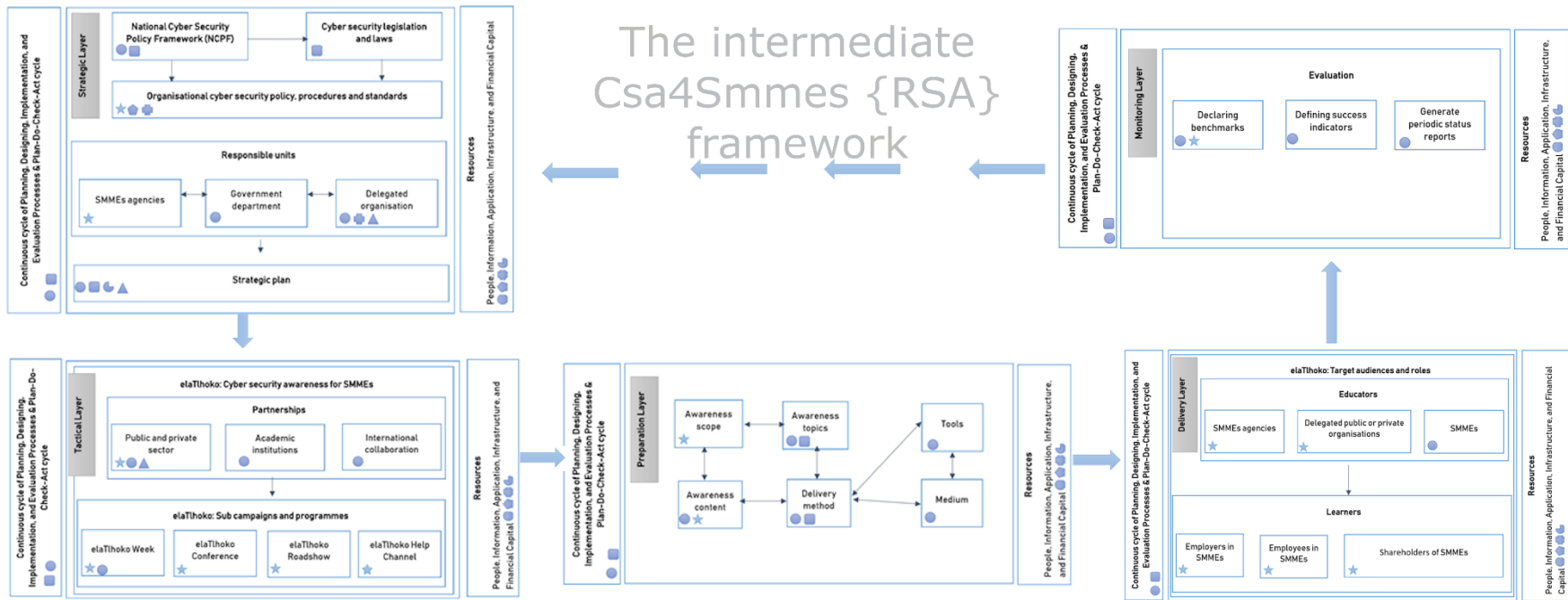


Figure 4-12: The intermediate Csa4Smmes {RSA} framework

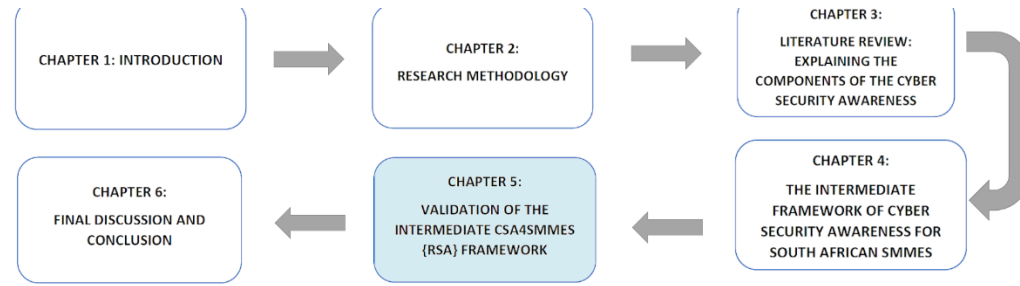
## 4.5 SUMMARY

The intermediate Csa4Smms {RSA} framework contributes to improving the culture of cyber security awareness in South Africa, specifically within SMMEs. If this intermediate Csa4Smms {RSA} framework is implemented, it will introduce the *elaTlhoko* campaign, including its sub-campaigns and programmes. This campaign will help the South African government in distributing cyber security awareness within SMMEs across the country. Furthermore, this campaign will provide a tailored cyber security awareness message to suitable target audience groups within South African SMMEs. As a result, the fourth sub-research question (SRQ4) has been answered by identifying factors related to characteristics and challenges faced by SMMEs.

This chapter has also answered the fifth sub-research question (SRQ5) by developing the intermediate Csa4Smms {RSA} framework tailored for the South African community of SMMEs.

The next chapter focuses on validating the intermediate Csa4Smms {RSA} framework.

# CHAPTER 5: VALIDATION OF THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK



<b>CHAPTER 5: VALIDATING THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK</b>	5.1	INTRODUCTION	5.2	OVERVIEW OF CHAPTER 5
	5.3	DEMONSTRATION AND EVALUATION IN DESIGN SCIENCE RESEARCH METHODOLOGY	5.4	DEFINING AN EXPERT
	5.5	INTERVIEW PROCESS	5.6	FINDINGS FROM INTERVIEWS
	5.7	A FRAMEWORK FOR CYBER SECURITY AWARENESS IN SMALL, MEDIUM AND MICRO ENTERPRISES (SMMEs)	5.8	SUMMARY

# 5 VALIDATION OF THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK

## 5.1 INTRODUCTION

The previous chapter introduced the intermediate Csa4Smmes {RSA} framework. This chapter aims to validate the intermediate Csa4Smmes {RSA} framework. As shown in Figure 5-1, demonstration and evaluation are the last phase of the DSRM approach. The evaluation phase is an important component of the research process (Hevner et al., 2004).

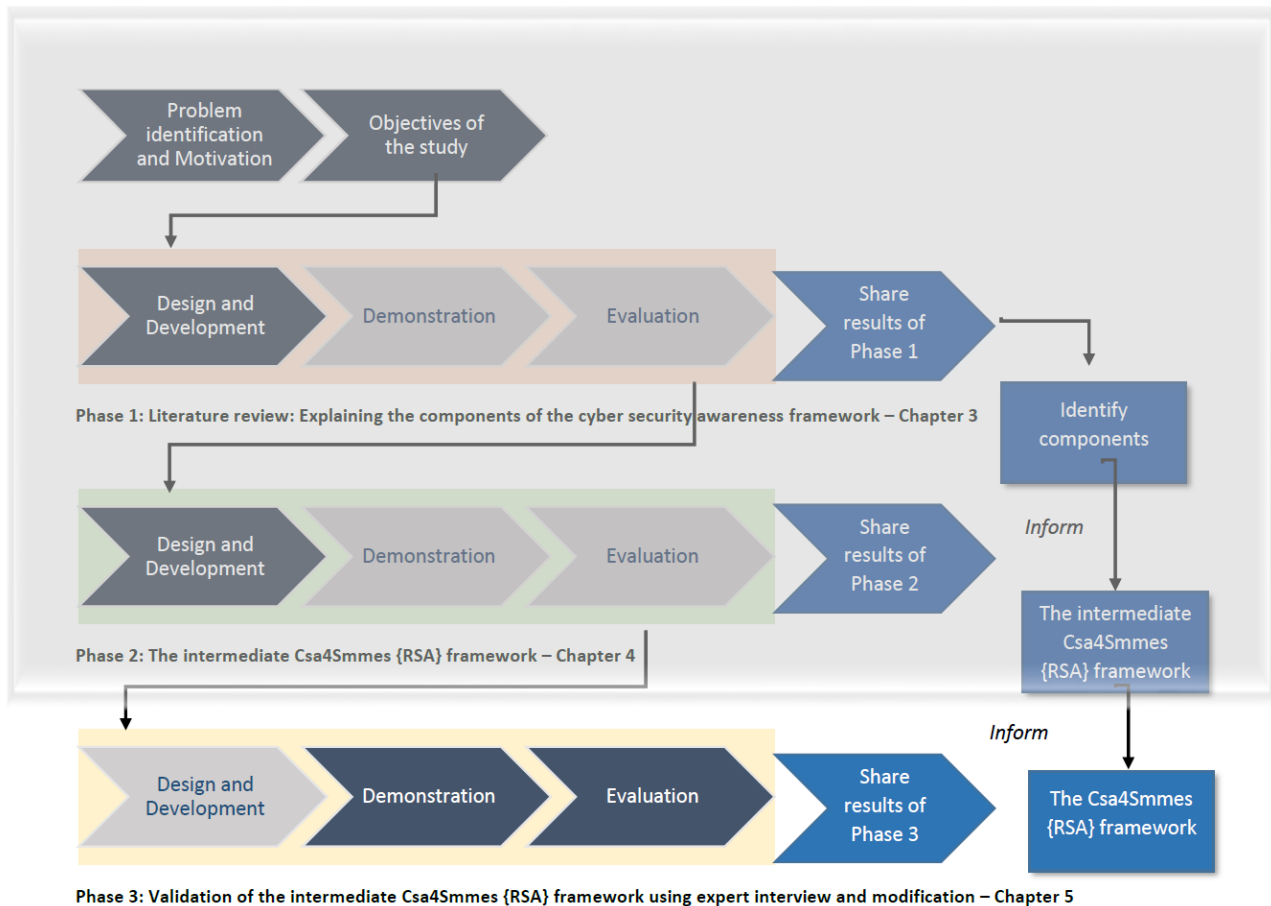


Figure 5-1: DSRM Process - Phase 3: The validation of the intermediate Csa4Smmes {RSA} framework.



Feedback obtained during the demonstration and evaluation process will be discussed, assessed and applied to validate and improve the intermediate Csa4Smmes {RSA} framework. This feedback from expert reviewers was used to answer the main research question of the study, namely:

*What would constitute a cyber security awareness framework for South African SMMEs?*

## **5.2 OVERVIEW OF CHAPTER 5**

Chapter 5 begins with the discussion of the demonstration and evaluation method utilised in this study (Section 5.3); then follows a discussion regarding the identification and selection of experts to demonstrate and evaluate the intermediate Csa4Smmes {RSA} framework (Section 5.4). Thereafter, the discussion regarding the process of interviewing experts and obtaining, interpreting and presenting experts' findings is covered in Section 5.5. In addition, a discussion is provided concerning the experts' recommendations and views of the intermediate Csa4Smmes {RSA} framework (Section 5.6). Recommendations and views of expert reviews are applied to constitute the Csa4Smmes {RSA} framework (Section 5.7), while the summary of the chapter is provided in Section 5.8.

The next sub-section provides a discussion regarding the evaluation process followed to identify and select experts to evaluate the intermediate Csa4Smmes {RSA} framework.

## **5.3 DEMONSTRATION AND EVALUATION IN DESIGN SCIENCE RESEARCH METHODOLOGY**

In DSRM, it is important to demonstrate and evaluate the developed artefact in order to determine how well the artefact solves the identified problem (March & Smith, 1995). Therefore, in this study, demonstration and evaluation of the intermediate Csa4Smmes {RSA} framework were conducted in parallel through expert reviews and used as an approach to validate the intermediate Csa4Smmes {RSA} framework, because properly implemented evaluation methods could be used to demonstrate the quality of an artefact (Hevner et al., 2004). Different groups of expert reviewers (primary and secondary) were

asked the same set of interview questions for both demonstrating and evaluating the intermediate Csa4Smmes {RSA} framework.

The next sub-section provides a discussion regarding the identification and selection of experts who will review the intermediate Csa4Smmes {RSA} framework.

## **5.4 DEFINING AN EXPERT**

An expert can be defined as an individual who possesses an adequate amount of knowledge which can be used to make critical decisions and solve any related subject matter problem at a given time (Chi, Glaser, & Farr, 1988; Maclellan & Soden, 2003). Expert reviews are usually included in research to review the outcome or artefact of the project (Jansen & Hak, 2005). The primary role of expert reviewers is to identify and disclose possible glitches of the presented artefact during the evaluation process (Holbrook, Krosnick, Moore, & Tourangeau, 2007). In addition, a researcher can use expert reviews to evaluate the usefulness of an artefact without including an end-user (Carlsson et al., 2011). Therefore, knowledge from expert reviewers can be used to demonstrate and evaluate the intermediate Csa4Smmes {RSA} framework.

### **5.4.1 Defining validation phase**

The intermediate Csa4Smmes {RSA} framework was demonstrated and evaluated by a variety of experts with knowledge regarding cyber security awareness mainly for the community of South African SMMEs. Individual components of the intermediate Csa4Smmes {RSA} framework were demonstrated and evaluated using a set of factors which will be discussed in the next sub-section.

Demonstration can be defined as a process of using the artefact in solving a problem through a variety of methods, while evaluation can be defined as the act to show how the artefact addresses the problem and meets defined objectives. In addition, the evaluation phase is used to evaluate the usefulness of an artefact and that process aids to validate the artefact (Herselman & Botha, 2015). Validation can be defined as the act of proving that something is correct, useful and at the acceptable standard. In this study, experts evaluated the framework to validate the usefulness of the framework. Thus, in the

evaluation phase the validation is reached. Therefore, going forward when referring to the term validation it should be noted that demonstration and evaluation phases forms part of validation process.

#### **5.4.2 Selection process**

In this study, expert reviewers were identified and grouped into primary and secondary expert reviewers. The primary expert reviewers included people from the cyber security domain and the science and technology awareness domain. The capabilities from both domains were important for the validation of the intermediate Csa4Smme {RSA} framework because these expert reviewers were in positions of valuable knowledge related to the components of the framework.

The secondary experts included people from SMME management and operation from one SMME in information technology and one SMME in environmental management. These expert reviewers were important to demonstrate the intermediate Csa4Smme {RSA} framework for usability and simplicity.

Both the primary and secondary expert reviewers answered the same interview questions because the knowledge from both domains provided an ability to cover all components of the intermediate Csa4Smme {RSA} framework from different perspectives which promoted collaboration and inclusiveness. This approach was followed because both primary and secondary experts gained extensive experience that impacts the capability for observing, organizing, representing, and understanding information within their industry (National Research Council, 2000). Therefore, feedback from secondary experts was used to demonstrate the intermediate Csa4Smme {RSA} framework, while feedback from primary experts was used for demonstration and evaluation. These expert reviewers were identified and grouped based on knowledge base related to either one or more of the fields below. For the sake of the validation phase the primary experts were seen as experts with knowledge in:

- Cyber security (minimum of five years of experience)
- Cyber security awareness (minimum of five years of experience)

- Cyber security practice or research (minimum of five years of experience)
- Science and technology awareness (minimum of seven years of experience)

For the sake of the validation phase, secondary experts were seen as experts with experience in:

- Working closely with SMMEs (including science centres) or SMME management and operations (minimum of seven years of experience)
- Cyber security awareness (not compulsory but advantageous)

To identify primary expert reviewers with knowledge in cyber security practice and awareness, the Council for Scientific and Industrial Research (CSIR) was approached. The CSIR was selected because of its speciality within the cyber security field in terms of research, practice and awareness. The CSIR has a specialised research group that has developed a cyber security awareness programme for educating people around the usage of the internet and social networks to enhance their awareness level.

In this study, two to four expert reviewers within the CSIR were required to attend one-on-one interviews to validate the intermediate Csa4Smmes {RSA} framework. The signed permission letter from the CSIR was obtained and submitted along with the ethical clearance application to UNISA.

In addition, primary expert reviewers with knowledge in science and technology awareness, the South African Agency for Science and Technology Advancement (SAASTA) was approached. SAASTA was selected because it “is a business unit of the National Research Foundation (NRF) with the mandate to advance public awareness, appreciation and engagement of science, engineering, innovation and technology in South Africa” (SAASTA, n.d). In addition, the organisation was selected because of its footprint in all provinces of South Africa in terms of awareness and relationships with individuals, organisations (SMMEs included) and science centres.

In this study, two to four expert reviewers within the SAASTA were required to attend one-

on-one interviews to validate the intermediate Csa4Smmes {RSA} framework. The signed permission letter from the SAASTA was obtained and submitted along with the ethical clearance application to UNISA.

To identify the secondary expert reviewers with experience in SMME management and operation, a search was conducted over the internet, utilising Google Search, LinkedIn and other relevant social media platforms. The experts were identified, obtained their contact details with their approval and sent a formal invitation, consent form and other related documents for them to voluntarily participate in the study. Two to four expert reviewers within the SMMEs were required to attend one-on-one interviews to demonstrate the intermediate Csa4Smmes {RSA} framework.

The expert reviewers were excluded based on their decision regarding participation in the study. In addition, experts were also excluded in the study if their contact details were not accessible, unable to obtain approval from respective organisations or an expert did not reply to the invitation.

Six expert reviewers were selected to validate the intermediate Csa4Smmes {RSA} framework using semi-structured interviews. Background information of selected expert reviewers is summarised in Table 5-1. The selected expert reviewers received the consent form and information sheet through an email, and the consent forms were signed to confirm their involvement in validating the intermediate Csa4Smmes {RSA} framework. The method of collecting data was conducted in compliance with the Policy on Research Ethics of the University of South Africa and in line with the approval ethical clearance.

**Table 5-1: Background information about expert reviewers**

<b>Expert review</b>	<b>Category</b>	<b>Knowledge domain</b>	<b>Years of experience</b>
Expert reviewer 1	Primary expert review	Cyber security	5 – 10
Expert reviewer 2	Primary expert review	Awareness	10 – 15

<b>Expert review</b>	<b>Category</b>	<b>Knowledge domain</b>	<b>Years of experience</b>
Expert reviewer 3	Primary expert review	Cyber security	5 – 10
Expert reviewer 4	Secondary expert review	SMME	5 – 10
Expert reviewer 5	Primary expert review	Awareness	10 – 15
Expert reviewer 6	Secondary expert review	SMME	5 – 10

**5.5 INTERVIEW PROCESS**

The selected expert reviewers comprised two cyber security practitioners and researchers, two experts with science and awareness experience (primary expert reviewers) and two experts in SMME management and operations (secondary expert reviewers). These expert reviewers were interviewed to provide the necessary ideas that could be used to improve the intermediate Csa4Smms {RSA} framework. These interviews were conducted virtually using Microsoft Teams, and the sessions were recorded and interpreted. Moreover, these experts were interviewed based on the layers and components of the intermediate Csa4Smms {RSA} framework.

These interviews were conducted to validate the components of the intermediate Csa4Smms {RSA} framework. The process of validating the framework was integrated into a single interview session for each expert reviewer. The feedback obtained from selected secondary expert reviewers (SMMEs) was used to demonstrate the intermediate Csa4Smms {RSA} framework. The feedback obtained from the selected primary expert reviewers from the CSIR and SAATA were used to demonstrate and evaluate the intermediate Csa4Smms {RSA} framework. In addition, results from the evaluation phase were used to validate intermediate Csa4Smms {RSA} framework which resulted into a Csa4Smms {RSA} framework.

### 5.5.1 Interview guide

The components of the intermediate Csa4Smmes {RSA} framework were validated based on the following evaluation factors defined by the researcher:

- *Importance*: This factor validates if a certain component or layer has a great significance or worth for enhancing cyber security awareness for South African SMMEs.
- *Clarity*: This factor validates if a certain component or layer is clear, coherent, intelligible and well represented.
- *Structure (grouping and flow)*: This factor validates if a certain component or layer is highly organised and arranged in a definite pattern.
- *Relevance*: This factor validates if a certain component within a layer is at a state of being closely connected to or appropriate for others.
- *Inclusivity*: This factor validates if a certain component is at a state of quality of coverage with a range of subjects or areas.
- *Applicability (Easy to apply or use by South African SMMEs)*: This factor validates if a certain component is at a state of quality of being relevant or appropriate.
- *Rigour*: This factor validates if a certain component is at a state of quality of being extremely detailed and careful.

These factors were used to provide guidance in the process of conducting semi-structured interviews with expert reviewers. To validate the intermediate Csa4Smmes {RSA} framework, these factors were considered to determine the quality of the framework and the components within each layer. The next sub-section provides a list of the interview questions used.

### 5.5.2 Interview questions

The selected expert reviewers were interviewed based on formulated interview questions to validate and provide additional components that were missing from the intermediate Csa4Smme {RSA} framework. Interview questions were developed and aligned with the layers, components and the complete structure of the intermediate Csa4Smme {RSA} framework.

These interview questions aimed to validate the overall structure of the intermediate Csa4Smme {RSA} framework based on information from expert reviewers which provided an opportunity for improving the framework. In addition, these interview questions were asked to obtain confirmation that the intermediate Csa4Smme {RSA} framework would contribute to enhancing cyber security awareness within South African SMMEs.

Semi-structured interviews were conducted using the interview guide as discussed. Interview questions to be asked per interviewee might differ at given times to allow the interviewer to focus and probe deeper into a certain topic (David & Sutton, 2004; Kajornboon, 2005). In this study, the same set of questions was asked; however, a flexible approach was followed because a response for a certain question could cover other sets of questions depending on the response from the expert reviewer.

The following interview questions were asked to obtain information from expert reviewers:

#### **General**

In your opinion, do you think using layers to divide the intermediate Csa4Smme {RSA} framework is effective?

If the intermediate Csa4Smme {RSA} framework is implemented, do you think it will contribute to enhancing cyber security awareness within the community of South African SMMEs?



Do you have any other comments and suggestions regarding the intermediate Csa4Smmes {RSA} framework?

How can the intermediate Csa4Smmes {RSA} framework be tailored to meet the needs of South African SMMEs?

### **The strategic layer**

What is your verdict regarding the components of the strategic layer (intermediate Csa4Smmes {RSA} framework) in terms of evaluation factors?

### **The tactical layer**

What is your verdict regarding the components of the tactical layer (intermediate Csa4Smmes {RSA} framework) in terms of evaluation factors?

### **The preparation layer**

What is your verdict regarding the components of the preparation layer (intermediate Csa4Smmes {RSA} framework) in terms of evaluation factors?

### **The delivery layer**

What is your verdict regarding the components of the delivery layer (intermediate Csa4Smmes {RSA} framework) in terms of evaluation factors?

### **The monitoring layer**

What is your verdict regarding the components of the monitoring layer (intermediate Csa4Smmes {RSA} framework) in terms of evaluation factors?

## **5.5.3 Stages of validating the framework**

The intermediate Csa4Smmes {RSA} framework was validated during the following stages with related timelines as shown in Table 5 2:

**Table 5-2: Validation timelines**

<b>Stage</b>	<b>Timeframe</b>
<i>Data collection:</i> Collecting data to validate the intermediate Csa4Smmes {RSA} framework by interviewing experts.	Four to six weeks
<i>Transcribing, analysing and reporting:</i> Analysing, interpreting and summarising feedback acquired from experts regarding the intermediate Csa4Smmes {RSA} framework.	Two to three weeks
<i>Updating the framework:</i> Using feedback from interviews to improve the intermediate Csa4Smmes {RSA} framework.	Four to seven weeks

All interviews conducted were recorded, transcribed and uploaded onto Atlas.ti to analyse data, based on the process of thematic data analysis. Codes and themes emerged from the process of thematic data analysis are as shown in thematic network diagrams. Thematic networks are web-like diagrams that provide a summary of key themes establishing a piece of text (Attride-Stirling, 2001). Furthermore, thematic networks are suitable for a systematic presentation of qualitative analyses because they simplify critical relationships within data and help to illustrate why a specific interpretation is acceptable (Spiegelhalter, 2014).

## **5.6 FINDINGS FROM INTERVIEWS**

The demonstration and evaluation phases were important phases in the study to determine its trustworthiness. The demonstration and evaluation phases were applied to ensure validity, reliability and rigour by using data collected from primary sources to

validate the intermediate Csa4Smmes {RSA} framework which was constructed based on data collected from secondary sources (Morse, Barrett, Mayan, Olson, & Spiers, 2002). These phases improved the trustworthiness of the results as follows:

- *Credibility*: Credibility refers to a state where the research findings reflect the reality of the contributors. Credibility provides an environment that allows other individuals to be familiar with processes taken within the research study (Thomas & Magilvy, 2011). To ensure credibility in the study, data was collected through multiple data sources.
- *Dependability*: Dependability provides an environment where another researcher can obtain the same research findings by analysing the collected raw data in the study (Thomas & Magilvy, 2011). To ensure dependability of the research findings, data was collected from both primary source using interviews that were conducted with expert reviewers to validate the intermediate Csa4Smmes {RSA} framework and secondary source by conducting a systematic literature review.
- *Confirmability*: Confirmability provides an environment where research findings can be confirmed and be unbiased from the motivations and perceptions of a researcher. Research findings should instead be driven, based on the contributions of participants (Thomas & Magilvy, 2011). Expert reviewers were interviewed to confirm results from the systematic literature. Responses from the expert reviewers were used to validate and improve the intermediate Csa4Smmes {RSA} framework.
- *Transferability*: Transferability provides an environment where the research findings can be transferred from one sample of a study to another. It also enables the research findings to be applicable to other studies with the same contexts (Thomas & Magilvy, 2011). This study can be regarded transferrable because the results of the study and the research process followed in this study can be adopted in a study with a similar setting.
- *Authenticity*: Authenticity provides an environment where the researcher displays

a variety of realities with fairness and openness (Guba, 1990). To ensure authenticity of the research findings, expert reviewers were identified and selected, based on their knowledge (related to cyber security awareness and practice, science and technology awareness, and SMME management and operations) to validate the components of the intermediate Csa4Smmes {RSA} framework. These expert reviewers contributed valuable information which improved the Csa4Smmes {RSA} framework.

This section provides discussions regarding the responses from six interviewed expert reviewers. The responses were analysed using the thematic analysis approach and interpreted through the hermeneutic cycle to validate the components of the intermediate Csa4Smmes {RSA} framework. Thematic analysis helps with the process of analysing data to provide meaningful information which is understandable, and the hermeneutic cycle includes the process of reading, analysing, reflective writing and interpretation in a rigorous manner (Laverly, 2003). These approaches were implemented to validate the intermediate Csa4Smmes {RSA} framework.

The following process of data analysis in the thematic analysis process was considered (Braun & Clarke, 2006):

- *Phase 1: Familiarising with data* – In this phase, data obtained from expert interviewers was transcribed and continuously read to search for meaning, insight and patterns. During this phase, ideas were formulated to identify possible patterns which could be used to formulate initial codes.
- *Phase 2: Generating initial codes* – In this phase, ideas formulated were used to generate an initial list of codes about the data. This phase was conducted using a software program called Atlas.ti which allows collating of relevant data into codes.
- *Phase 3: Searching for themes* – In this phase, initial codes were analysed and refocused by categorising different codes into potential themes. Generated codes were analysed for potential combinations and data associated with each code was reviewed.

- *Phase 4: Reviewing themes* – In this phase, all generated themes were analysed to refine themes. Data associated with themes was used to formulate meaning. In addition, initial thematic network diagrams were developed to virtualise the formulated themes.
- *Phase 5: Defining and naming themes* – In this phase, the thematic network diagrams and themes were analysed to generate clear definitions, names and story for each theme. Data related to each theme was retrieved to conduct and write a comprehensive analysis.
- *Phase 6: Producing the report* – In this phase, a comprehensive report about the analysis of data from expert interviews was generated to provide insight into the data and to answer the research questions of the study.

### 5.6.1 Components of the strategic layer

The interviewed expert reviewers were asked to share their verdict regarding components of the strategic layer in terms of the evaluation factors.

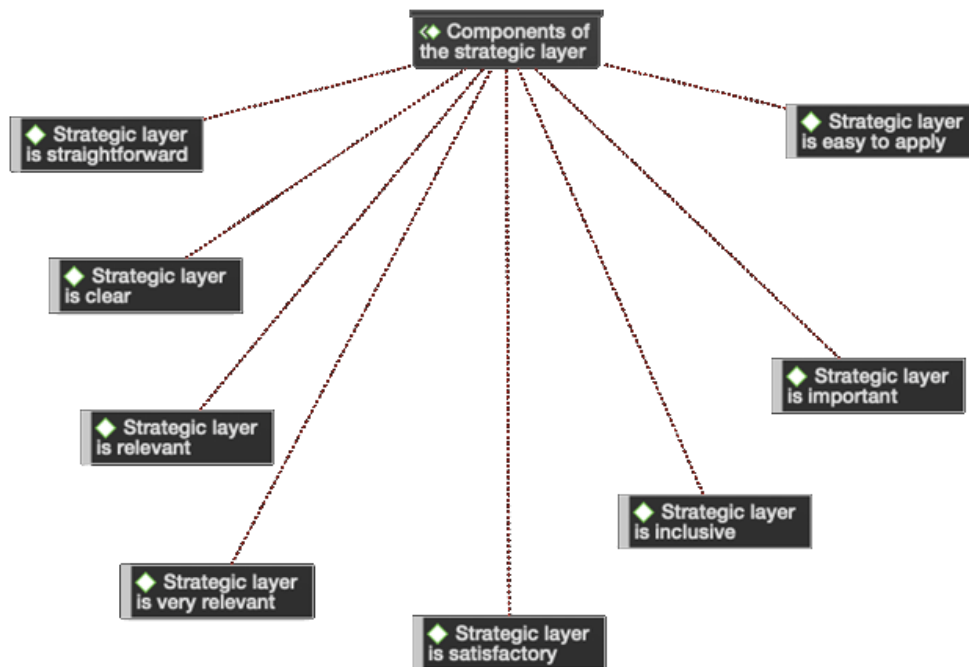


Figure 5-2: Components of the strategic layer - thematic network diagram

As shown in Figure 5-2, derived codes from interviews were categorised together to validate the intermediate Csa4Smmes {RSA} framework. In Figure 5-2, the components of the strategic layer were assessed and resulting codes, as shown in the figure, were generated based on feedback from the expert reviewers.

Expert reviewer 2 suggested traditional leadership be added to the strategic layer under responsible unit. Traditional leadership such as kingships, queenships and principal traditional leaders “are the rightful leaders of their own constituencies, which are communities in their areas of jurisdiction” (South African Government News Agency, 2017). Expert reviewer 2 also indicated that there are a lot of places that still operate under traditional leadership. In addition, Expert reviewer 2 stated that “You have to go to them and ask permission to penetrate their community with your activities...” Therefore, a new block which will be added in the strategic layer under the “Responsible” unit represent traditional leaders. Traditional leaders can collaborate with government and other responsible units to assist in supporting, promoting and evaluating cyber security awareness in SMMEs located within communities that operate under their leadership.

Expert reviewer 4 suggested the inclusion of state-owned enterprises which is already covered under government departments. Expert reviewer 1 stated that the CyberSecurity Hub could be integrated in the intermediate Csa4Smmes {RSA} framework. However, it had already been incorporated as the government department within responsible unit (see section 4.4.4.3.d). Expert reviewer 3 suggested that the relationship between NCPF and cyber security legislation and laws should be clarified or simplified. However, the relationship between the block of NCPF and cyber security legislations and laws will remain the same, because the NCPF aims to develop, evaluation and amend existing substantive and procedural laws to evade misalignment (Sutherland, 2017). Expert reviewer 5 suggested the integration of the National Development Plan which defines long-term goals. However, the National Development Plan 2030 does not address cyber security in detail (National Planning Commission, 2011). Expert reviewer 5 also suggested the inclusion of the implementation plan which was covered under the strategic plan.

Moreover, all the expert reviewers stated that the strategic layer was well placed and it was good that the framework had the government as an umbrella because if the awareness initiatives did not support a government strategy, the awareness initiative would become invalid. Then it would become difficult to get support from the government. Expert reviewer 1 also stated that the strategic layer it is very relevant because “everything flows from top to down, so whatever happens on the grass root must always support the top strategy. So, I think it is important and it helps to have the strategic layer in place”. Expert reviewer 5 stated that government department(s) was well-placed because it was centralised and it interacted with delegated business units and SMMEs.

### 5.6.2 Components of the tactical layer

The expert reviewers were asked to share their verdict regarding components of the tactical layer in terms of the evaluation factors.

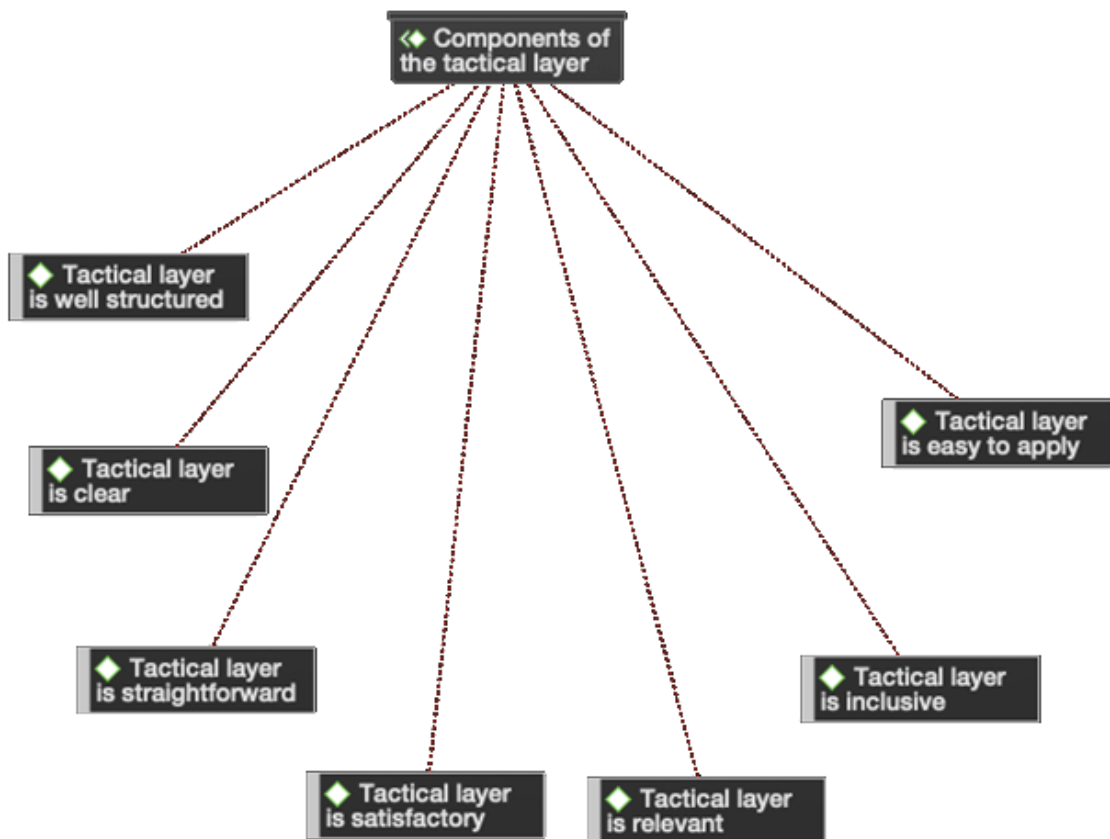


Figure 5-3: Components of the tactical layer - thematic network diagram

As shown in Figure 5-3, derived codes from interviews were categorised together to validate the intermediate Csa4Smmes {RSA} framework. In Figure 5-3, the components of the tactical layer were assessed and resulting codes, as shown in the figure, were generated, based on feedback from the expert reviewers.

Expert reviewer 5 suggested an inclusion of research institutions because they were different from academic institutions. Therefore, a new block will be added under “Partnerships” to represent research institutions. Expert reviewer 2 agrees with the usage of identified partnerships and stated that the public and private sector and academic institutions covered almost all organisations we have in the country. They also suggested that the usage of international collaborators is a great idea because our country can learn best practices from countries that are doing well. Expert reviewer 2 concluded by stating that the usage of the *elaTlhoko* campaign in the tactical layer was “very relevant and it’s needed, because awareness is key”.

In addition, Expert reviewer 4 stated that the *elaTlhoko* campaign was a catchy phrase, and that all identified partnerships were clear and straightforward. Then expert review 4 also emphasised that the inclusion of the train-the-trainer approach was important because SMMEs could relate much better with one another. Expert reviewer 1 and expert reviewer 2 suggested that the *elaTlhoko* campaign could be integrated with the National Cyber Security Awareness Month (NCSAM) and the National Science Week (NSW) respectively.

These suggestions can be integrated to support the *elaTlhoko* campaign because some of the *elaTlhoko* sub-campaigns can be conducted during those specified periods (NCSAM and NSW). However, new blocks for these integrations (NCSAM and NSW) will not be added as components in the framework.

Expert reviewer 3 and expert reviewer 6 agreed that the tactical layer highlighted all the important aspects and it was clear, including the relationship between partnerships and campaign, well-structured and relevant. Expert reviewer 5 suggested stakeholder engagement with stakeholders and target audience. However, the *elaTlhoko* Conference covered a suggestion made. Expert reviewer 5 also suggested renaming the “Help



Channel” to “Help Centre”. Therefore, the *elaTlhoko* Help Channel will be renamed to *elaTlhoko Help Centre* because it can be conducted through virtual services using multiple channels such as emails, social media, self-service, live chats and more. In addition, Expert reviewer 4 suggested the campaign be continuous and virtual because of limitations caused by Covid-19. However, the suggestion is covered by the *elaTlhoko* Help Channel.

### 5.6.3 Components of the preparation layer

These expert reviewers were asked to share their verdict regarding components of the preparation layer in terms of the evaluation factors.

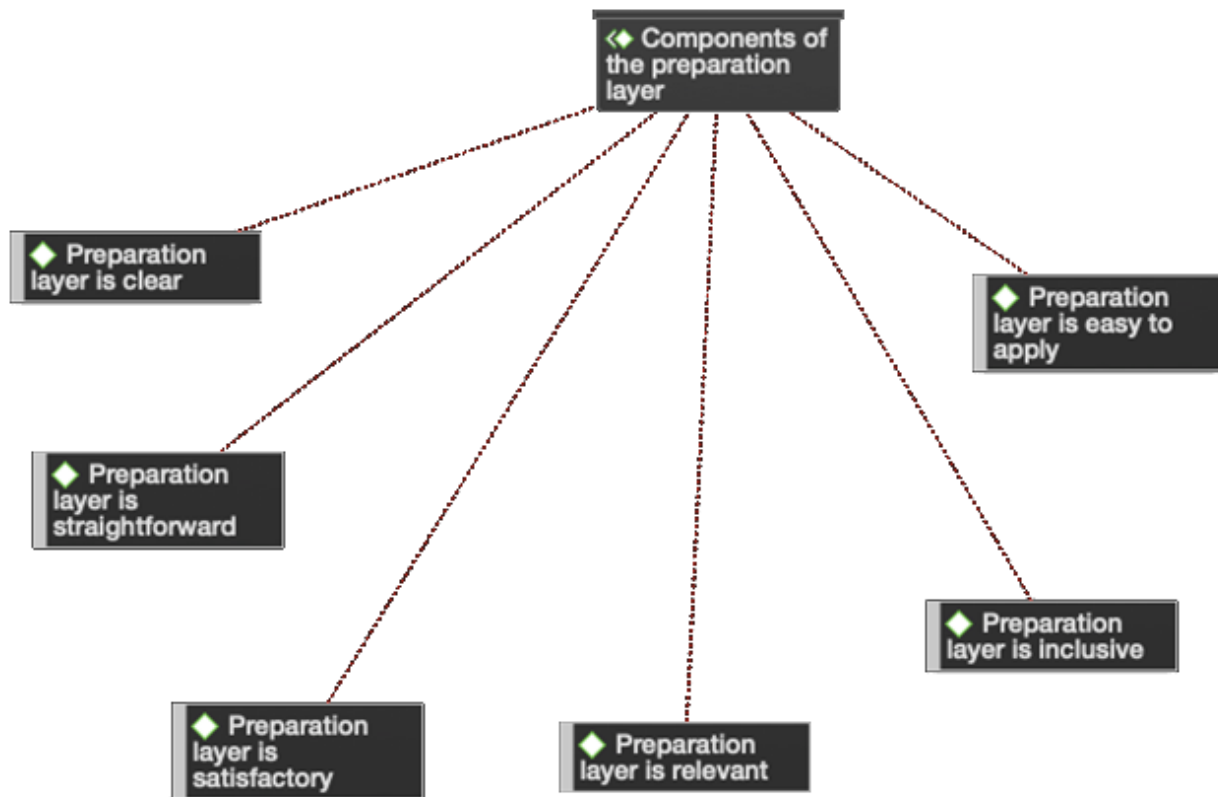


Figure 5-4: Components of the preparation layer - thematic network diagram

As shown in Figure 5-4, derived codes from the interviews were categorised together to validate the intermediate Csa4Smme {RSA} framework. In Figure 5-4, the components of the preparation layer were assessed and resulting codes, as shown in the figure, were generated, based on feedback from the expert reviewers.

Expert reviewer 1 stated that awareness content had to be updated, where necessary, to avoid repeating the awareness content for the same target audience because “cyber threats keep on changing, there are new threats, there are new viruses out there, and criminals keeps on coming up with new ways”. To respond to the suggestion, the monitoring layer is for evaluating the effectiveness of the cyber security awareness by means of the *elaTlhoko* campaign and the intermediate Csa4Smme {RSA} framework. In addition, the process of evaluation and monitoring can assist SMMEs to continuously improve the existing awareness campaign.

Expert reviewer 2 stated that when conducting awareness, “we also have to filter in the issue of language. We need to go to where people are. We need to reach them at their own language”. Expert reviewer 2 also indicated that these communities could be reached by utilising multiple channels including local radio stations which cater for all languages in the country. Therefore, awareness content should be delivered using a desired language of the target audience and a block will be added to the preparation layer to represent multiple languages.

Expert reviewer 3 suggested a sequential flow for components under the preparation layer. However, all components of the preparation layer are aligned with one another; thus, applying sequential flow will limit the relationship among components. These relationships provide flexible flow among components because the cyber security awareness process is iterative and continuous.

Expert reviewer 5 commented that for every awareness topic to be delivered, there scoping exercises had to be related to it. Expert reviewer 5 also stated that a delivery method was dependent. However, the selected delivery method has effects on the selected topic and content because every delivery method comes with its limitations.

Expert reviewer 4 emphasised that the preparation layer was straightforward, and easy to interpret and follow. In addition, expert reviewer 6 demonstrated an understanding of all components presented in the preparation layer and liked that the cyber security awareness content delivered through the framework was not a “one book fits all”, meaning it is tailored, based on specific requirements.

#### 5.6.4 Components of the delivery layer

The expert reviewers were asked to share their verdict regarding components of the delivery layer in terms of the evaluation factors.

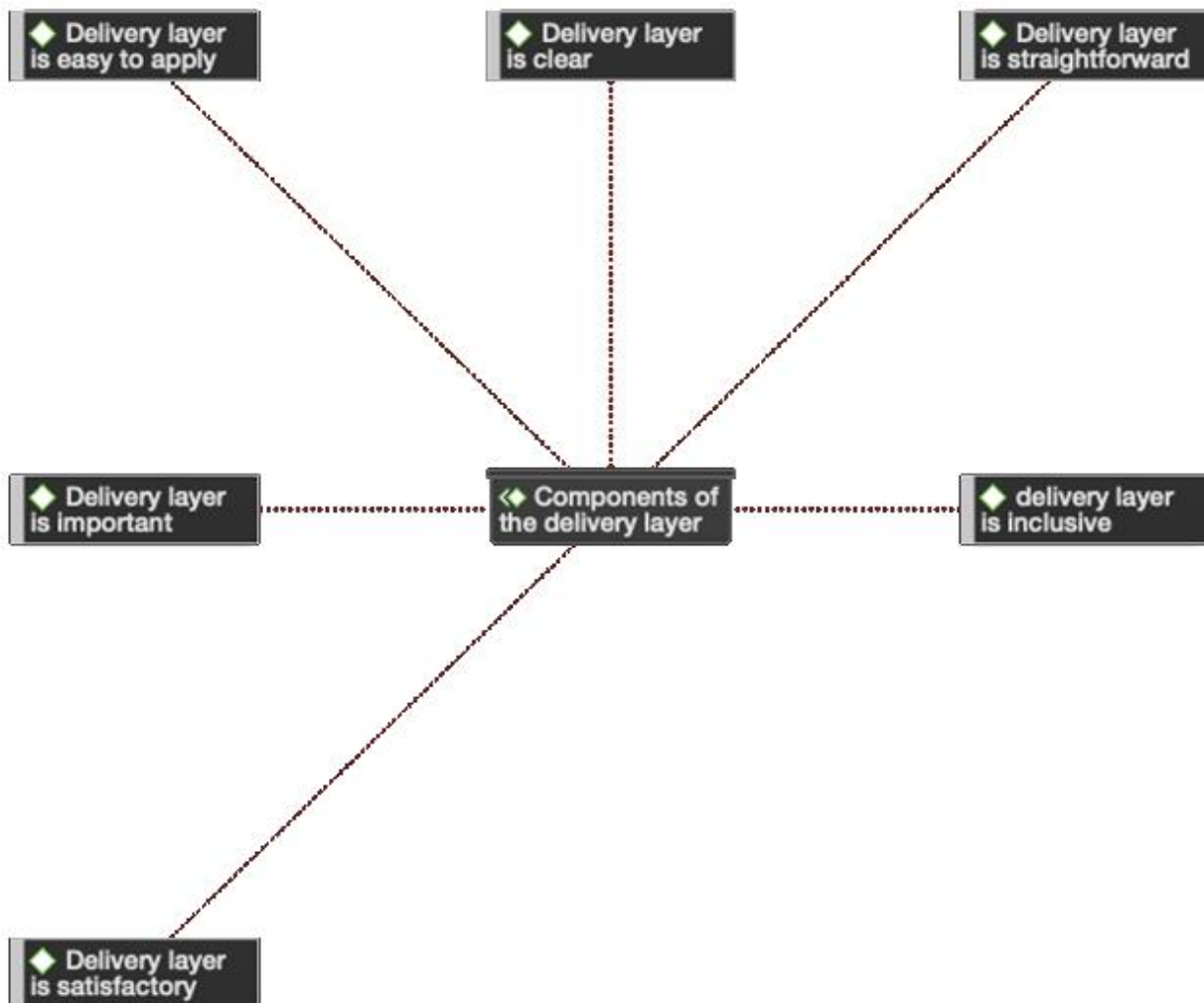


Figure 5-5: Components of the delivery layer - thematic network diagram

As shown in Figure 5-5, the derived codes from interviews were categorised together to validate the intermediate Csa4Smms {RSA} framework. In Figure 5-5, the components of the delivery layer were assessed and resulting codes, as shown in the figure, were generated, based on feedback from the expert reviewers.

Expert reviewer 2 stated that “there are people in communities (registered and unregistered structures such as non-profit organisations also known as NPOs) that are already playing these roles”. In addition, expert reviewer 1 suggested the involvement of NPOs in the framework. These individuals could play the educator role by integrating *elaTlhoko*'s cyber security awareness activities into their existing programmes which they ran within communities. Therefore, a block that represents *NPOs and individuals* will be included as a target audience playing the educator role.

All of the expert reviewers agreed that the delivery layer was satisfactory. Expert reviewer 6 agreed that including delegated organisations from both the private and public sectors to play the educator role would help to provide initial training for fellow educators because they were well-trained and cyber security awareness was part of their daily responsibilities. However, Expert reviewer 5 suggested a renaming of the educator role and learner role to *facilitators* and *participants* respectively. This suggestion will be implemented accordingly.

### **5.6.5 Components of the monitoring layer**

The expert reviewers were asked to share their verdict regarding components of the monitoring layer in terms of the evaluation factors.

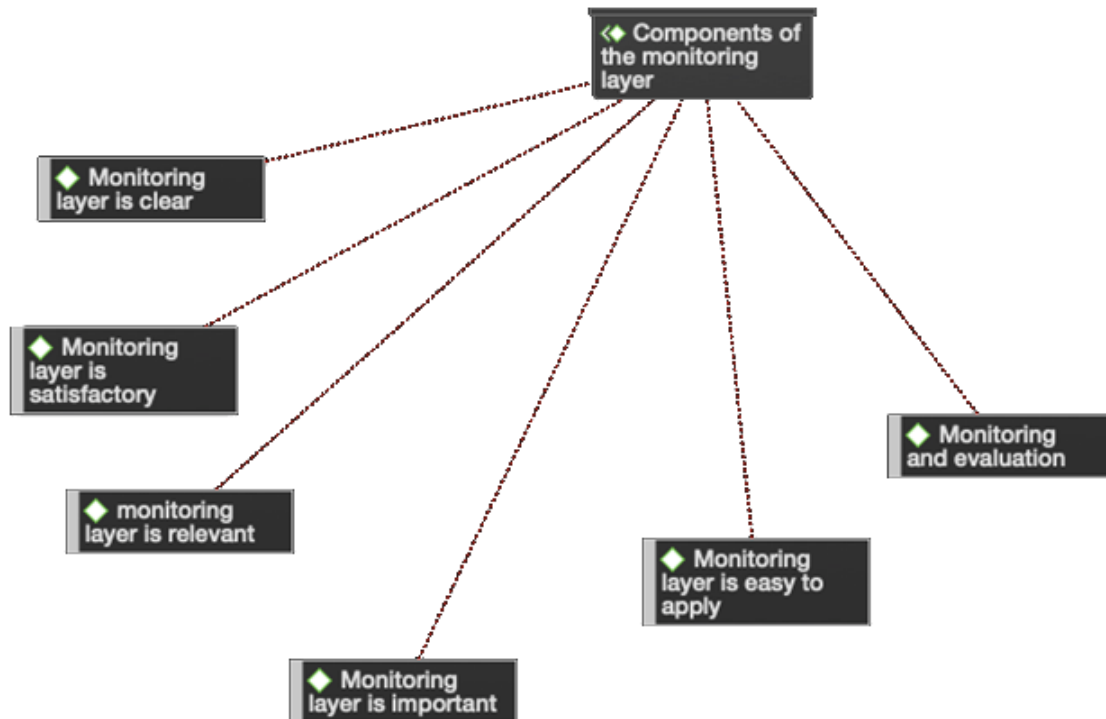


Figure 5-6: Components of the monitoring layer - thematic network diagram

As shown in Figure 5-6, derived codes from interviews were categorised together to validate the intermediate Csa4Smmes {RSA} framework. In Figure 5-6, the components of the monitoring layer were assessed and resulting codes, as shown in the figure, were generated, based on feedback from the expert reviewers.

Expert reviewer 5 suggested the layer be renamed to “Monitoring and evaluation” and to add a component that represented the process of collection, collation and analysis. This component will be added as recommended. This process includes gathering data using a variety of methods, assembling raw data to produce standardised data, as well as inspecting, cleaning and transforming that standardised data into useful information which can be used for reporting.

Expert reviewer 6 emphasised the importance of conducting monitoring because “in everything we do, we should monitor, analyse and observe for new developments”. Expert reviewer 2 and expert reviewer 6 emphasised that without the monitoring layer,

one would not be able to know if one was making positive progress or not, either in the short or long term. Expert reviewer 1 and expert reviewer 6 agreed that the monitoring layer made sense because all components within the layer were the most important components required when running campaigns.

Expert reviewer 1 suggested an integration to generate an official cyber security related statistic (Stats SA) in the form of a report which could be used by government to measure the impact of the intermediate Csa4Smmes {RSA} framework. The monitoring layer already provided reports that could be generated at different levels of the intermediate Csa4Smmes {RSA} framework.

### 5.6.6 Comments and suggestions

Expert reviewers were asked to share their comment regarding the overall structure of the intermediate Csa4Smmes {RSA} framework, its possible contribution, and how it be tailored further for South African SMMEs.

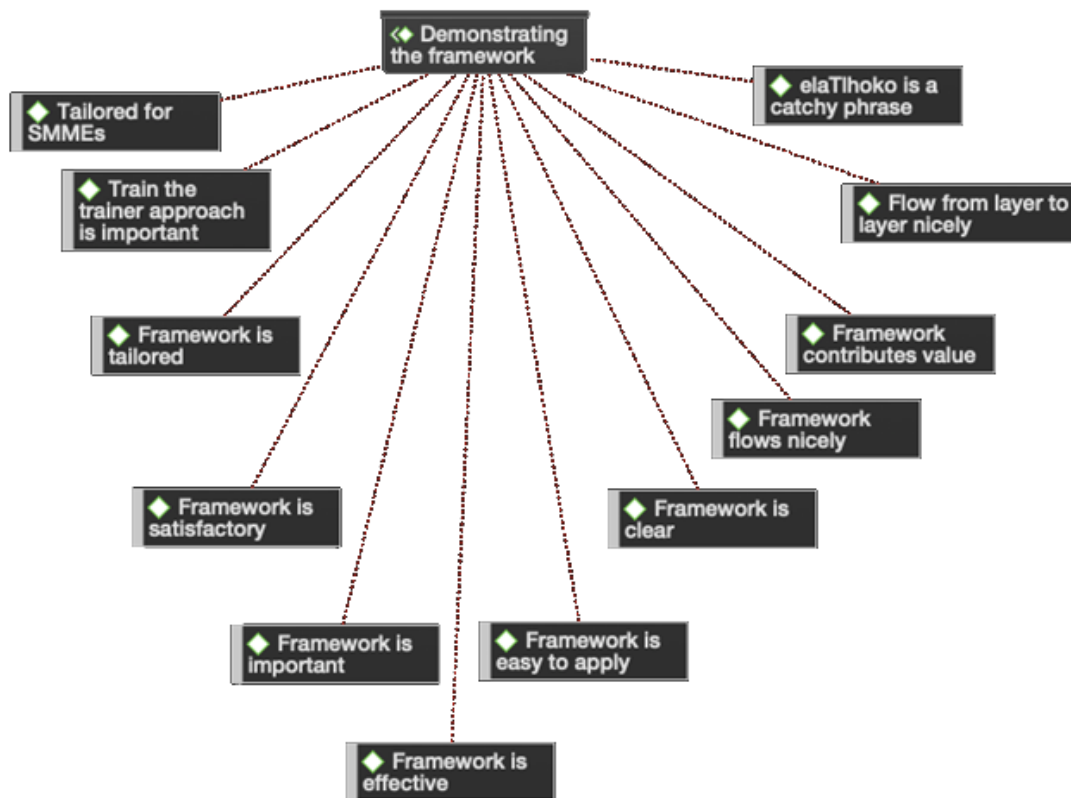


Figure 5-7: Demonstration of the intermediate Csa4Smmes {RSA} framework - thematic network diagram

As shown in Figure 5-7, derived codes from interviews were categorised together to demonstrate the intermediate Csa4Smmes {RSA} framework. In Figure 5-7, the intermediate Csa4Smmes {RSA} framework was assessed and resulting codes, as shown in the figure, were generated, based on feedback from the secondary expert reviewers (SMMEs). These generated codes were then used to label, organise, and analyse qualitative data to identify different concepts and relationship in between. Based on the thematic network diagram (Figure 5-7), feedback while demonstrating the intermediate Csa4Smmes {RSA} framework was graphically represented. Based on Figure 5-7, the proposed *elaTlhoko* campaign was found to be a catchy phrase. The secondary expert reviewers also mentioned that the intermediate Csa4Smmes {RSA} framework was clear, satisfactory, easy to apply, important, tailored for SMMEs and the flow between layers was well-presented. In addition, it was mentioned that the intermediate Csa4Smmes {RSA} framework would contribute value to SMMEs.

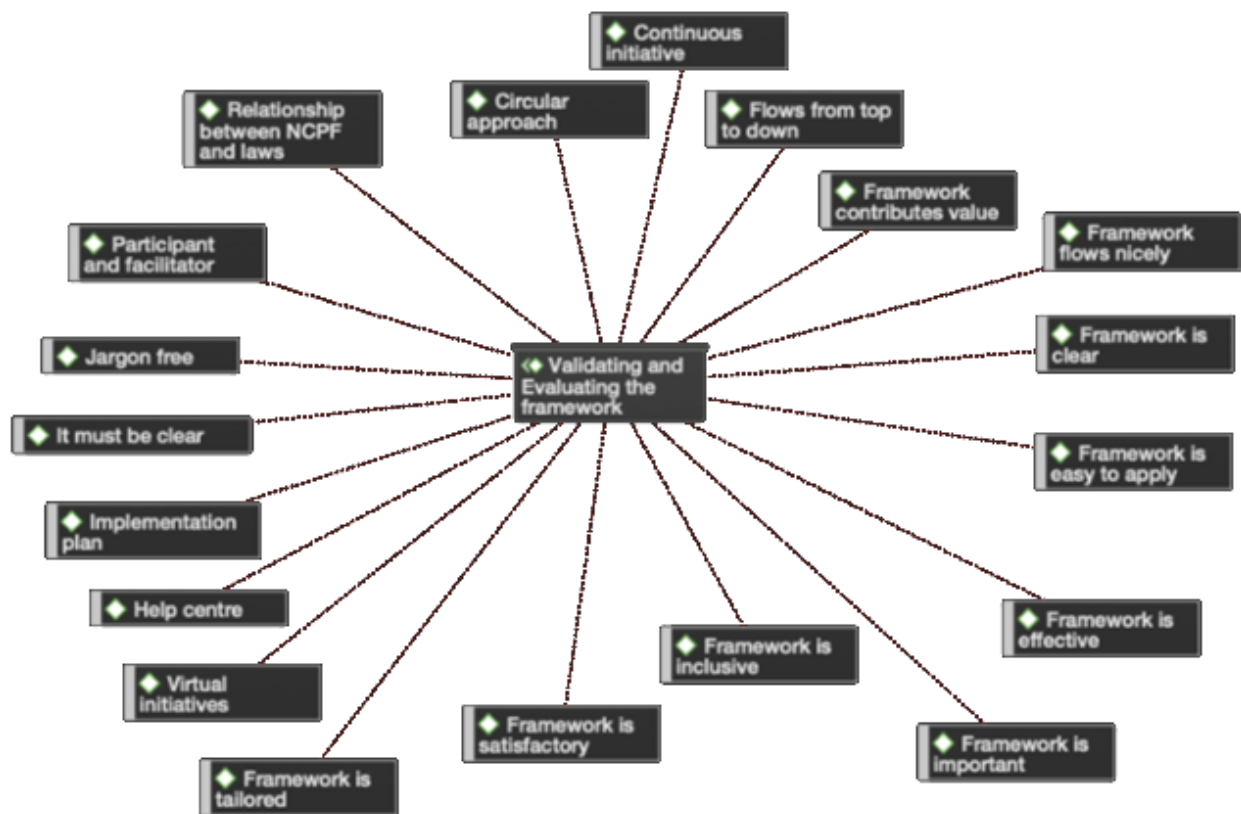


Figure 5-8: Validation of the intermediate Csa4Smmes {RSA} framework - thematic network diagram

As shown in Figure 5-8, derived codes from interviews were categorised together to evaluate the intermediate Csa4Smmes {RSA} framework. In Figure 5-8, the intermediate Csa4Smmes {RSA} framework was assessed and resulting codes, as shown in the figure, were generated, based on feedback from both the primary and secondary expert reviewers. These generated codes were then used to label, organise, and analyse qualitative data to identify different concepts and relationship in between. Based on the thematic network diagram, recommendations made to the intermediate Csa4Smmes {RSA} framework were graphically represented. Based on Figure 5-8, the intermediate Csa4Smmes {RSA} framework was clear, easy to apply, satisfactory, important, effective, inclusive, tailored for SMMEs, and the flow between layers was well-presented.

In addition, it was mentioned that the intermediate Csa4Smmes {RSA} framework would contribute value within SMMEs. However, expert reviewers suggested additional components that could be added to the intermediate Csa4Smmes {RSA} framework. Additional components, as shown in Figure 5-8 and Figure 5-9, will be discussed in the next sub-section.

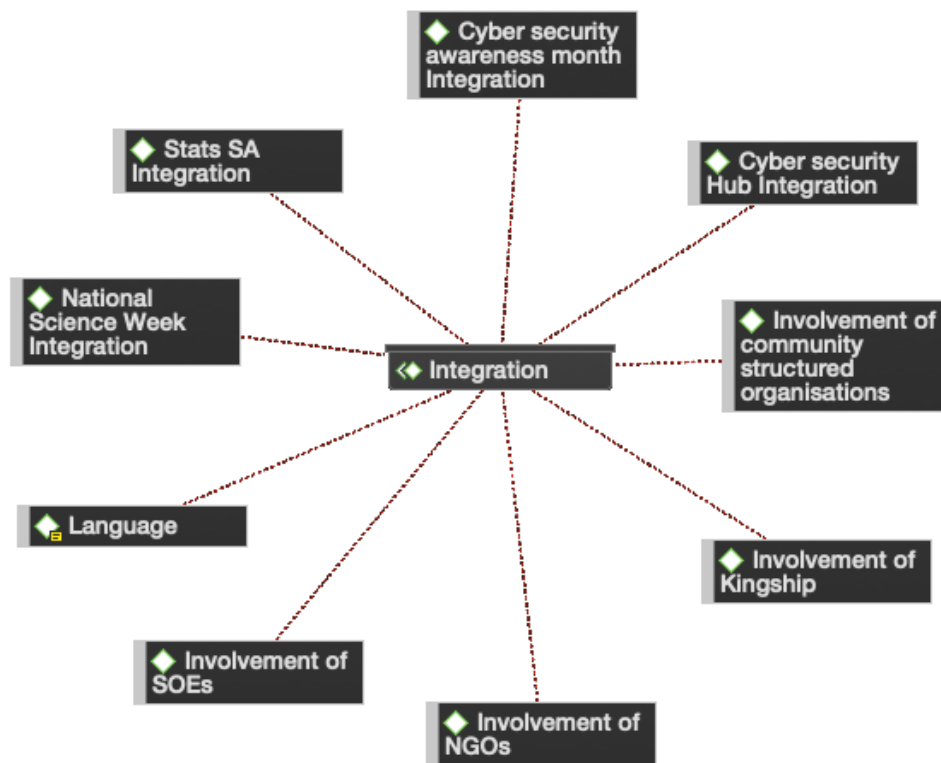


Figure 5-9: Integration for the intermediate Csa4Smmes {RSA} framework - thematic network diagram



As shown in Figure 5-9, derived codes from interviews were categorised together to validate the intermediate Csa4Smms {RSA} framework. In Figure 5-9, the components of the intermediate Csa4Smms {RSA} framework were assessed and resulting codes, as shown in the figure, were generated, based on feedback from the expert reviewers. According to Figure 5-9, the expert reviewers suggested various components that could be integrated into the intermediate Csa4Smms {RSA} framework. These suggested components include Statistics South Africa, Cyber Security Hub, Cyber Security Awareness Month, National Science Week, community-structured organisations, non-profit organisations, state-owned organisations, traditional leadership and the variety of languages.

Expert reviewer 2 and expert reviewer 3 stated that every South African SMME had to align the cyber security policy and awareness by aligning themselves with the NCPF and other South African national laws and legislation related to cyber security because it helps with tailoring cyber security awareness. Expert reviewer 2 stated that “SMMEs should look at what they need to protect about their own businesses”. Expert reviewer 4 stated that including contributions from SMMEs in the framework would help to address the needs of South African SMMEs. Expert reviewers 1, 5 and 6 stated that the intermediate Csa4Smms {RSA} framework had to be clear, simplified and consist of as less jargon as possible.

Expert reviewer 2 also stated that the layers of the intermediate Csa4Smms {RSA} framework provides a clear guideline or direction to rollout the project. In addition, expert reviewer 1 stated that “all layers of the intermediate Csa4Smms {RSA} framework make sense because going through all of them together, you could tell there is a flow”. Expert reviewer 1 emphasised that the intermediate Csa4Smms {RSA} framework was an iterative cycle, understandable and broken down pretty nicely. Expert reviewer 3 suggested that a relationship among the monitoring layer and the other layers should be clarified and reflected on the overall structure of the intermediate Csa4Smms {RSA} framework. Therefore, numerical values will be added to the layers of the framework to improve the flow and structure of the framework.

Expert reviewer 3 concluded by stating that all layers were clear and fitted nicely with one another in sequence. Expert reviewers 3 and 6 stated that the flow improved the applicability of the framework, since it started with recommended ways of conducting cyber security awareness and the alignment with NCPF and legislation.

Expert reviewer 2 stated that by taking the *elaTlhoko* initiative to communities one is directly impacting and enhancing awareness within SMMEs. Expert reviewer 2 concluded by stating that the intermediate Csa4Smms {RSA} framework could empower SMMEs in terms of enhancing cyber security awareness and assisting them to prepare themselves for the Fourth Industrial Revolution (4IR). Expert reviewer 5 commented that it was important to do awareness-related projects because awareness was one of the missing links related to the work conducted by government. Expert reviewer 6 stated that in everything, awareness was an initial phase. In addition, expert reviewer 6 agreed that the framework would improve cyber security awareness for SMMEs.

All recommendations were assessed and applied if necessary. However, the process of data collection stopped when insight regarding the components of the intermediate Csa4Smms {RSA} framework was saturated (Creswell, 2014). It means that gathering new data during interviews did not reveal new insight into the components of all layers.

## **5.7 A FRAMEWORK FOR CYBER SECURITY AWARENESS IN SMALL, MEDIUM AND MICRO ENTERPRISES (SMMEs)**

The intermediate Csa4Smms {RSA} framework was validated using feedback from expert reviewers. Their suggestions were applied to the framework and as a result, the Csa4Smms {RSA} framework is presented in Figure 5-10. Based on the feedback from the expert reviewers, components listed in Table 5-3 were added or modified as per their recommendations which resulted in the Csa4Smms {RSA} framework. These components are indicated with a pink star in Figure 5-10. Table 5-3 below clarifies the layers of the Csa4Smms {RSA} framework, the components added or modified in the Csa4Smms {RSA} framework and the action taken towards the component (added, removed or modified).

**Table 5-3: List of components added, removed or modified to form the Csa4Smmes {RSA} framework**

<b>Layer</b>	<b>Component</b>	<b>Action</b>
Strategic layer	Traditional leaders	Added
Tactical layer	Research institutions	Added
Tactical layer	<i>elaTlhoko</i> Help Centre	Modified
Preparation layer	Languages	Added
Delivery layer	NPOs and individuals	Added
Delivery layer	Facilitators (educator's role)	Modified
Delivery layer	Participants (learner's role)	Modified
Monitoring layer	Collection, collation and analysis	Added
Monitoring layer	Monitoring and evaluation	Modified

Therefore, the components listed in Table 5-3 were applied to formulate the Csa4Smmes {RSA} framework. In addition, numbers 1-5 were included to portray the flow of the Csa4Smmes {RSA} framework.

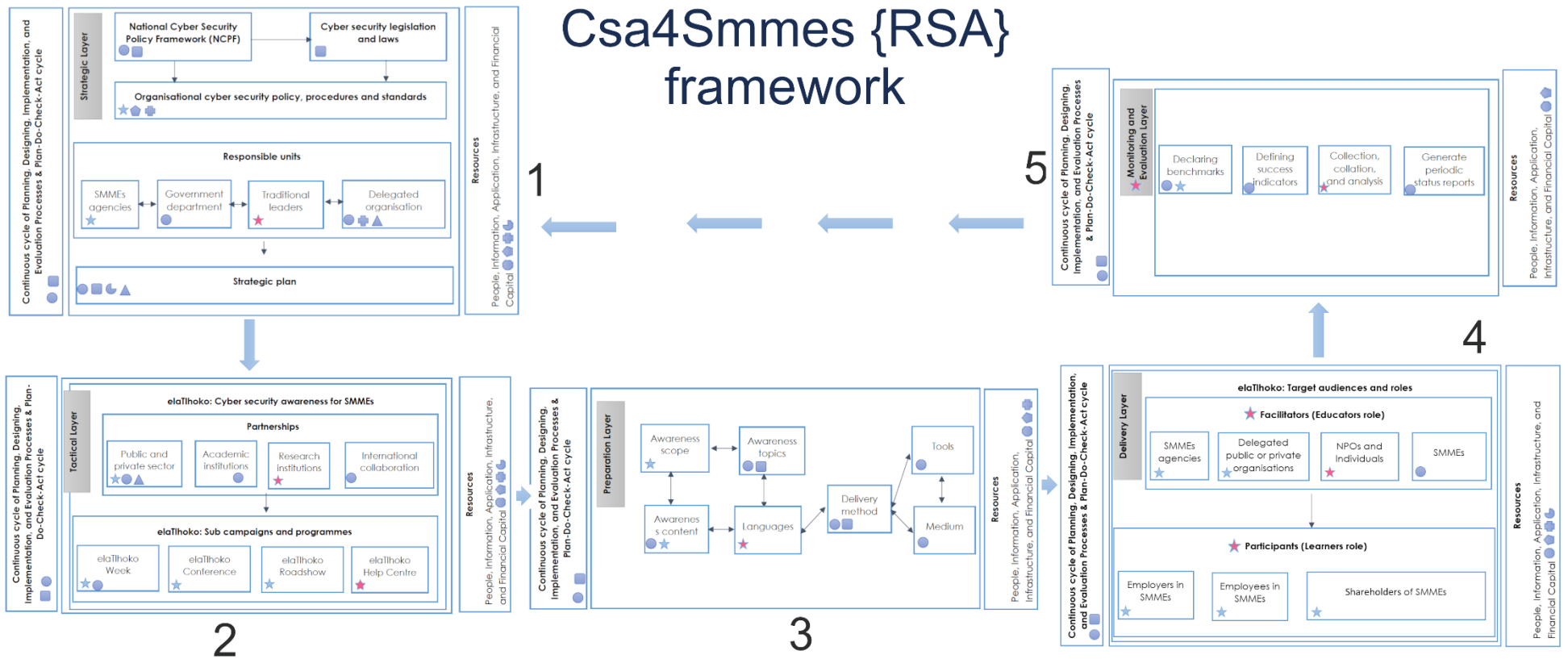


Figure 5-10: A framework for cyber security awareness in SMMEs

## 5.8 SUMMARY

This chapter provided a discussion regarding the process of validating the intermediate Csa4Smmes {RSA} framework. Feedback from expert reviewers was used to improve and confirm the applicability of the Csa4Smmes {RSA} framework. Comments and suggestions made by the expert reviewers were considered to improve the framework in terms of adding, removing or modifying components within the layers of the Csa4Smmes {RSA} framework which led to traditional leadership being added as an additional component in the strategic layer.

Research institutes were added as an additional component in the tactical layer. In addition, the *elaTlhoko* Help Channel was renamed to become the *elaTlhoko* Help Centre in the tactical layer. Language was added as an additional component in the preparation layer.

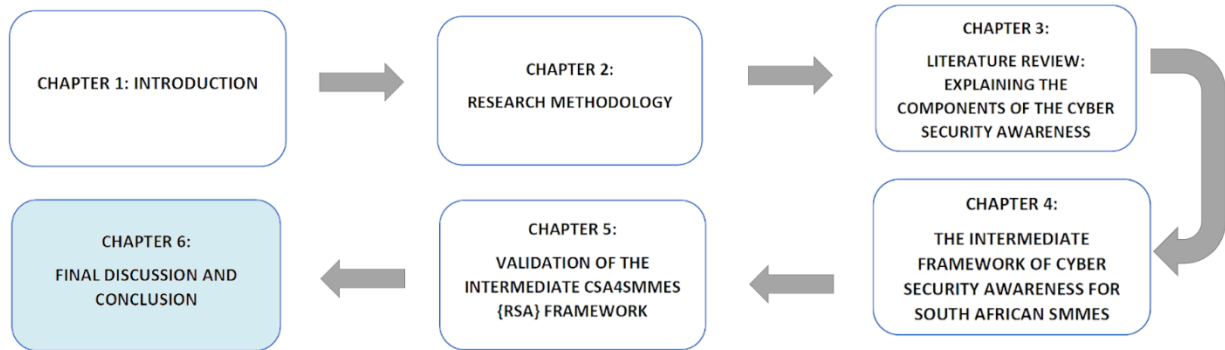
The “NPOs and individuals” block was added as an additional component in the delivery layer. Also in the delivery layer, the educator’s and learner’s role components were renamed to *facilitators* and *participants* respectively.

The “Collection, collation and analysis” block was added as an additional component in the monitoring layer.

Therefore, these changes have been applied to construct the Csa4Smmes {RSA} framework (Figure 5-10) which is different from the intermediate Csa4Smmes {RSA} framework (Figure 4-12).

The Csa4Smmes {RSA} framework was produced as an artefact because the DSRM mainly focused on creating or advancing an artefact to improve its efficiency. Consequently, this chapter answered the main research question and achieved the main objective of the study by developing the Csa4Smmes {RSA} framework tailored for the South African community of SMMEs. The next chapter provides a summary of the research study.

# CHAPTER 6: FINAL DISCUSSION AND CONCLUSION



<b>CHAPTER 6: FINAL DISCUSSION AND CONCLUSION</b>	6.1	INTRODUCTION	6.2	OVERVIEW OF CHAPTER 6
	6.3	REVIEW OF THE RESEARCH PROBLEM	6.4	REFLECTION ON RESEARCH QUESTIONS
	6.5	SUMMARY OF THE RESEARCH DESIGN	6.6	SUMMARY OF RESEARCH CHAPTERS
	6.7	RESEARCH CONTRIBUTION	6.8	LIMITATIONS
	6.9	FUTURE RESEARCH	6.10	CONCLUSION

## **6 FINAL DISCUSSION AND CONCLUSION**

### **6.1 INTRODUCTION**

The main objective of the research study was to develop a cyber security awareness framework for South African SMMEs. The research study applied the design science research methodology to develop the Csa4Smmes {RSA} framework. This chapter answers research questions and provides summary on research study in terms of findings, design, recommendations, reflections, and conclusion.

### **6.2 OVERVIEW OF CHAPTER 6**

This chapter begins with a review regarding the research problem of the study (Section 6.3). In Section 6.4, a reflection of research questions of the study is provided. A summary of the research design and chapters is covered in Section 6.5 and Section 0 respectively. Contribution and limitations of the research study is covered in Section 6.7 and Section 6.8 respectively. Future research is covered in Section 6.9, while conclusion is covered in Section 6.10.

The next sub section provides a discussion regarding the research problem of the study.

### **6.3 REVIEW OF THE RESEARCH PROBLEM**

Organisations regardless of size and nationality (including South African SMMEs) are depended on IT to boost services and sustain competitive advantage (Abawajy, 2014). IT provides opportunities for SMMEs to connect, communicate and collaborate with other parties globally to participate in broader markets and to be up to date with modern technology (Sami, 2016; Van de Haar, 2014).

SMMEs plays a significant role in the world economic growth because countries and economies depend on SMMEs for unique economic contributions through flexibility and innovation (Coertze, 2012; Le Roux, 2010; Koornhof, 2009; Sánchez et al., 2010). In addition, SMMEs are creating employment opportunities which improves the economy and reduces poverty in developing countries (Nichter & Goldmark, 2009; Sami, 2016). In

South Africa, there is a significant increase in SMMEs (Kent et al., 2016). However, SMMEs are vulnerable and increasingly targeted by cyber criminals due to financial constraints and limited or no security knowledge (Harris & Patten, 2014; PwC, 2020; Von Solms, 2015). SMMEs do not pay adequate attention to cyber security and their unsecured activities can critically impact the cyber security infrastructure of the country because SMMEs can also offer services to large organisations and government departments (Kent et al., 2016; Von Solms, 2015).

According to the systematic literature review conducted in this study, there is less research contribution towards cyber security awareness for South African SMMEs. It is important to provide tailored cyber security awareness for individuals within SMMEs because the country is vulnerable to cyber attacks (Department of Telecommunications and Postal Services, 2017). Cyber attacks are directed at businesses of all sizes including SMMEs which are impacted the most. These organisations are still not effectively prepared to prevent cybercrimes (PwC, 2016). In addition, they have insufficient knowledge concerning cyber threats and risks. These SMMEs are contributing towards the economy of the country. Therefore, the Csa4Smmes {RSA} framework was developed to provide cyber security awareness support for South African SMMEs because there is a need to create awareness for individuals within SMMEs.

#### **6.4 REFLECTION ON RESEARCH QUESTIONS**

The main research question of the study was the following:

*What would constitute a cyber security awareness framework for South African SMMEs?*

To respond to the main research question, the following sub-research questions (SRQs) were investigated:

- SRQ1: What current studies measure cyber security awareness for SMMEs in South Africa?



This sub-research questions identifies research studies that are focussing on cyber security awareness or information security awareness in South Africa. As shown in Table 3-3, selected research studies were analysed based on research focus, and this table portrays a shortage of academically based research studies on cyber security awareness for SMMEs. The general trend regarding security awareness in South Africa is mainly to measure information security awareness levels while considering knowledge, attitude, and behaviour of the target audience. Security awareness is presented mostly to school learners and university students. However, there is less focus on cyber security awareness for SMMEs.

- SRQ2: What existing cyber security awareness models or frameworks can be utilised for SMMEs?

This sub-research question identifies existing models and frameworks can be utilised or adopted to enhance the level of cyber security awareness within the community of SMMEs in South Africa. Based on the findings from the systematic literature review, none of the identified models and frameworks can be utilised completely and effectively for South African SMMEs without adjustments. As depicted in Table 3-5, it was discovered that models and frameworks mostly focus on organisational and national level respectively. In addition, most models and frameworks were proposed to enhance security awareness for internet users more than other target audiences. Models and frameworks as shown in Table 3-5 were adopted and analysed to identify building blocks that are required in constructing the intermediate Csa4Smme {RSA} framework.

- SRQ3: What components should be included in a cyber security awareness framework for SMMEs?

This sub-research question identifies components that are required for the intermediate Csa4Smme {RSA} framework. Selected models and frameworks as shown in Table 3-5 were analysed to identify components that are required for developing the intermediate Csa4Smme {RSA} framework. In addition, research studies included in Table 3-2, category 2, were also analysed to extrapolate

additional cyber security awareness related components. As shown in Figure 3-4, a list of components of cyber security awareness framework for SMMEs was developed based on research studies included in Table 3-2, category 2.

- SRQ4: What are the cyber security awareness needs within the South African community of SMMEs from a literature perspective?

This sub-research question identifies factors related to characteristics and challenges faced by SMMEs. SMME owners may have inadequate skills and knowledge to purposefully grow and manage their enterprises (South African Institute of Chartered Accountants, 2015). SMMEs must be provided with tailored cyber security awareness, based on company size, field of operation, and in house skills and resources. Therefore, the development of the intermediate Csa4Smms {RSA} framework (Figure 4-12) considered the uniqueness of SMMEs in terms of phases of development, characteristics and challenges faced which are different from large companies. These factors (which includes independently owned, resource constraints, limited education, vulnerability to cyber attacks, dependency on IT, and bad geographical location) were considered to meet needs for South African SMMEs.

- SRQ5: What would the intermediate Csa4Smms {RSA} framework comprise for the South African community of SMMEs?

This sub-research question aims to develop intermediate Csa4Smms {RSA} framework using identified components adopted from other research studies. The intermediate Csa4Smms {RSA} framework was constructed using the following building blocks: Four high-level stages of the NIST framework, Plan-Do-Check-Act (PDCA) cycle, process of planning, designing, implementation, and evaluation, five layers of cyber security awareness and education framework, and ten components of cyber security awareness framework. These identified components of cyber security awareness framework were assembled to develop the intermediate Csa4Smms {RSA} framework as shown in Figure 4-12.

- Main research question: What would constitute a cyber security awareness framework for South African SMMEs?

This main research question aimed to develop a cyber security awareness framework for South African SMMEs. The intermediate Csa4Smms {RSA} framework was validated by variety of experts with knowledge regarding cyber security awareness mainly for the community of South African SMMEs. Based on feedback from expert reviewers, certain components of the intermediate Csa4Smms {RSA} framework were added, removed, or modified. As a result, a cyber security awareness framework for South African SMMEs (Csa4Smms {RSA} framework) was developed as shown in Figure 5-10.

These research questions were used as a guideline that influences the research process of the study because formulating good research questions helps towards obtaining relevant answers. Therefore, all research questions were sufficiently answered.

## 6.5 SUMMARY OF THE RESEARCH DESIGN

In this study, the design science research methodology was utilised to develop the Csa4Smms {RSA} framework. DSRM is a research approach that answers research questions that are relevant to human problems through the development of innovative artefacts (constructs, models, methods and instantiations), thus contributing new knowledge to the body of scientific knowledge (Hevner & Chatterjee, 2010). In this study, guidelines of design science research methodology were applied in the study as follows:

- *Guideline 1 – Design as an artefact:* The study identified the components of cyber security awareness that are utilised to develop the Csa4Smms {RSA} framework that is tailored and appropriate for SMMEs (South African context).
- *Guideline 2 – Problem relevance:* The Csa4Smms {RSA} framework will provide a possible solution by contributing towards the cyber security culture for South African SMMEs because providing awareness for SMMEs might diminish the risk of successful cyber attacks associated to internet users.

- *Guideline 3 – Design evaluation:* The Csa4Smmes {RSA} framework was refined through the different phases, starting with the systematic literature reviews; identification of relevant cyber security components; developing and validating the framework through expert reviews. The Csa4Smmes {RSA} framework integrated all changes as suggested in each phase.
- *Guideline 4 – Research contribution:* The Csa4Smmes {RSA} framework is expected to provide valuable perceptions for the implementation of cyber security awareness within SMMEs in consideration of the South African context.
- *Guideline 5 – Research rigour:* To maintain rigour, different approaches such as systematic literature and expert interviews, were used to gather data from experts to validate the framework.
- *Guideline 6 – Design as a research process:* Some of the research questions were answered using systematic literature reviews to identify relevant components of cyber security awareness.
- *Guideline 7 – Communication of research:* The results of the research study have been published as conference papers and dissertation chapters.

The research study implemented the DSRM process (which consists of six activities) to explain the process followed by the study. The Csa4Smmes {RSA} framework was developed through all activities (Figure 1-2) and phases (Figure 2-1) of the DSRM process.

## **6.6 SUMMARY OF RESEARCH CHAPTERS**

### **Chapter 1: INTRODUCTION**

In Chapter 1, an introduction and background information of the research study was stated to motivate the problem statement. In addition, research questions, objectives, importance, motivation, brief methodology, ethical consideration, and chapter overview of the study was presented.

### **Chapter 2: RESEARCH METHODOLOGY**

In Chapter 2, the applied research design process was discussed. DSRM was applied to develop an artefact based on data from systematic literature review. In addition, interview data collection method was used to obtain data that was used for demonstrating and evaluating the artefact. In this chapter, ethical clearance of the research study was presented.

### **Chapter 3: LITERATURE REVIEW: EXPLAINING THE COMPONENTS OF THE CYBER SECURITY AWARENESS FRAMEWORK**

In Chapter 3, a systematic literature review was conducted to extrapolate components required to develop the intermediate Csa4SmmeS {RSA} framework. A list of components required to develop the intermediate Csa4SmmeS {RSA} framework was formulated. In addition, the systematic literature review process followed was presented as well.

### **Chapter 4: THE INTERMEDIATE FRAMEWORK OF CYBER SECURITY AWARENESS FOR SOUTH AFRICAN SMMEs**

In Chapter 4, characteristics and challenges faced by SMMEs were presented. In addition, the intermediate Csa4SmmeS {RSA} framework was developed based on identified characteristics of SMMEs, components formulated in Chapter 3, and other components adopted from other models and frameworks.

### **Chapter 5: VALIDATION OF THE INTERMEDIATE CSA4SMMEs {RSA} FRAMEWORK**

In Chapter 5, the intermediate Csa4Smms {RSA} framework was validated by expert reviewers during one-to-one interview sessions. The selection process of expert reviewers was presented. Based on feedback from expert reviewers, the intermediate framework was improved. As a result, the Csa4Smms {RSA} framework was developed.

## Chapter 6: FINAL DISCUSSION AND CONCLUSION

Chapter 6 provides a review of the research problem, reflection of research questions and objectives, and summary of the research design and research chapters. In addition, research contribution, limitations, future work, and conclusion of the research study was presented.

### **6.7 RESEARCH CONTRIBUTION**

The study aimed at developing a framework of cyber security awareness for South African SMMEs (Csa4Smms {RSA} framework). Design science research methodology was applied (through different phases and activities) to develop, demonstrate, evaluate, and validate a Csa4Smms {RSA} framework.

The new knowledge contribution supports the government and SMMEs because providing awareness for SMMEs might diminish the risk of successful cyber attacks associated to internet users (Muhirwe, 2016). In addition, the research study contributes towards the South African cyber security infrastructure because compromising cyber security for SMMEs can have a crucial influence towards the overall cyber security of the country (Von Solms, 2015).

The research study identified a research gap whereby a cyber security awareness study has not been conducted for South African SMMEs where a suitable model and framework for raising cyber security awareness for SMMEs in South Africa have been developed. In addition, the study identified that tailored and suitable models and frameworks which can be utilised to enhance cyber security awareness within the community of South African SMMEs has not been developed. Therefore, the main contribution of the research study was the development of a Csa4Smms {RSA} framework which will help SMMEs to improve their knowledge concerning cyber security and to prevent naive SMMEs from

becoming victims of cyber attacks (Ramírez, 2017). A Csa4Smme {RSA} framework will provide cyber security awareness for SMMEs to support the South African government in tackling the challenge of attaining a comprehensive security protection for the country.

The implementation of DSRM is likely to make an effective contribution to the body of knowledge within the research area through proper positioning and arrangement (Gregor & Hevner, 2013). Therefore, the Csa4Smme {RSA} framework makes a significant contribution to the body of knowledge by providing a framework that can be tailored and applied for enhancing cyber security awareness within the community of SMMEs. In addition, this framework contributes towards the industry by providing a collaborative platform for government (departments and state-owned enterprises), SMMEs agencies, delegated organisations (from private and public sector), and SMMEs to utilise in improving the level of cyber security awareness within South African SMMEs.

## **6.8 LIMITATIONS**

The research study is limited to South Africa in terms of identifying only academic research studies on cyber security awareness for SMMEs. The research study does not necessarily portray the views or practices of SMMEs in South Africa. The identified components of cyber security awareness were extrapolated from research studies that proposed cyber security awareness models and frameworks within the South African context. This research study was only focussed on developing and validating a cyber security awareness framework for SMMEs, but it was not implemented in SMMEs.

## **6.9 FUTURE RESEARCH**

Future research will focus on conducting fieldwork to implement a Csa4Smme {RSA} framework which might help in enhancing awareness levels within community of South African SMMEs. In addition, this fieldwork can be used as an additional method to validate and test the Csa4Smme {RSA} framework. A research study can be conducted to expand the framework in terms of developing a guideline (which includes templates and generic content which SMMEs can utilise) that can be handed out to target audience.

## 6.10 CONCLUSION

This research study focused on developing a Csa4Smme {RSA} framework that can be implemented within the community of South African SMMEs (Chapter 4). This framework was developed using components extrapolated from the systematic literature review (Chapter 3). Interviews were conducted with expert reviewers within the field of cyber security, science, and technology awareness, and in SMME management and operations. The feedback obtained from secondary experts was used to demonstrate the intermediate Csa4Smme {RSA} framework, while the feedback from the primary experts were used to demonstrate and evaluate the framework. In addition, the feedback from the evaluation phase was used to validate the intermediate framework which resulted into a Csa4Smme {RSA} framework (Chapter 5). In this chapter, a review of the research problem, reflection of research questions, summary of the research design, research contribution and limitations, and future research was provided.

A Csa4Smme {RSA} framework was developed to enhance cyber security awareness level within SMMEs in South Africa. SMMEs play a significant role towards growth of the South African economic. South African SMMEs do not have essential resources and knowledge to combat or reduce cyber threats. Therefore, it is important to help SMMEs to deal with cyber security related challenges. In conclusion, a Csa4Smme {RSA} framework can assist the government in reducing successful cyber attacks associated to internet users because cyber security awareness has been demonstrated to be an effective approach.



## 7 REFERENCES

- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248.  
<https://doi.org/10.1080/0144929X.2012.708787>
- Abawajy, J. H., Thatcher, K., & Kim, T. H. (2008). Investigation of stakeholders commitment to information security awareness programs. *Proceedings of the 2nd International Conference on Information Security and Assurance, ISA 2008*, 472–476.  
<https://doi.org/10.1109/ISA.2008.25>
- Abor, J., & Quartey, P. (2010). Issues in SME development in Ghana and South Africa. *Journal of Finance and Economics*, 39(6), 218–228.
- Adebesin, T. F. (2011). *Usability and accessibility evaluation of the digital doorway* [Master's dissertation, University of South Africa]. UNISA Institutional Repository.  
<http://hdl.handle.net/10500/4728>
- Agudelo, M. A. L., Jóhannsdóttir, L., & Davídsdóttir, B. (2019). A literature review of the history and evolution of corporate social responsibility. *International Journal of Corporate Social Responsibility*, 4(1), 1-23.
- Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science*, 72, 361-373. <https://doi.org/10.1016/j.procs.2015.12.151>
- Ahmad, N., Mokhtar, U. A., Fariza Paizi Fauzi, W., Othman, Z. A., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. N. (2019). Cyber security situational awareness among parents. *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018*. 1-3.  
<https://doi.org/10.1109/CR.2018.8626830>
- Al Awawdeh, S., & Tubaishat, A. (2014). An information security awareness program to address common security concerns in IT unit. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, 273–278.

<https://doi.org/10.1109/ITNG.2014.67>

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies*, 3(2), 8-29.

Aldawood, H., & Skinner, G. (2019a). Educating and raising awareness on cyber security social engineering: A literature review. *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018*. 62-68. <https://doi.org/10.1109/TALE.2018.8615162>

Aldawood, H., & Skinner, G. (2019b). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet*, 11(3), 73–89. <https://doi.org/10.3390/fi11030073>

Alghamdi, A. H. (2013). Adapting design-based research as a research methodology. *International Journal of Education and Research*, 1(10), 1–12. <http://ijern.com/journal/October-2013/27.pdf>

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, 42, 56–65. <https://doi.org/10.1016/j.cose.2014.01.005>

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *2014 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014*, 248–252. <https://doi.org/10.1109/ICITST.2014.7038814>

Amankwa, E., Loock, M., & Kritzinger, E. (2016). Enhancing information security education and awareness: Proposed characteristics for a model. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, 72–77. <https://doi.org/10.1109/InfoSec.2015.7435509>

Amjad, H. A. R., Naeem, U., Zaffar, M. A., Zaffar, M. F., & Choo, K. K. R. (2016). Improving security awareness in the government sector. *Proceedings of the 17th*

*International Digital Government Research Conference on Digital Government Research*, 1–7.

Andoh-Baidoo, F., Osatuyi, B., & Kunene, K. N. (2014). Architecture for managing knowledge on cyber security in sub-Saharan Africa. *Information Technology for Development*, 20(2), 140–164. <https://doi.org/10.1080/02681102.2013.832127>

Andreassen, T. (2011). *The practice of corporate social responsibility among small, micro and medium manufacturing enterprises in the Pietermaritzburg area and how this practice is influenced by their stakeholders* [Master's dissertation, University of KwaZulu-Natal]. UKZN Institutional Repository. <http://hdl.handle.net/10413/4962>

Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research*, 1(3), 385–405.

Babbie, E. (2020). *The practice of social research*. Cengage learning.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security*, 27(3). <https://doi.org/10.1108/ICS-07-2018-0080>

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *Conference: International Conference on Cyber Security for Sustainable Society*. 118–131.

Beaver, G. (2007). The strategy payoff for smaller enterprises. *Journal of Business Strategy*, 28(1), 11–17. <https://doi.org/10.1108/02756660710723161>

Beaver, G., & Jennings, P. (2005). Competitive advantage and entrepreneurial power: The dark side of entrepreneurship. *Journal of Small Business and Enterprise Development*, 12(1), 9–25.

Bedi, D. S. (2013). *Information security in hospitality SMMEs in the Cape Metropole area: Policies and measures in the online environment* [Master's dissertation, Cape Peninsula University of Technology]. CPUT Institutional Repository.

<http://etd.cput.ac.za/handle/20.500.11838/1693>

- Bloomberg. (2018, March 19). *Mark Zuckerberg under pressure over Facebook data breach*. MyBroadband. <https://mybroadband.co.za/news/security/252797-mark-zuckerberg-under-pressure-over-facebook-data-breach.html>
- Boell, S. K., & Cecez-Kecmanovic, D. (2010). Literature reviews and the hermeneutic circle. *Australian Academic & Research Libraries*, 41(2), 129-144.
- Borah, R., Brown, A. W., Capers, P. L., & Kaiser, K. A. (2017). Analysis of the time and workers needed to conduct systematic reviews of medical interventions using data from the PROSPERO registry. *BMJ Open*, 7(2). <http://dx.doi.org/10.1136/bmjopen-2016-012545>
- Botha, J. G., Eloff, M. M., & Swart, I. (2015). The effects of the PoPI Act on small and medium enterprises in South Africa. *Information Security for South Africa*, 1–8. <https://doi.org/10.1109/ISSA.2015.7335054>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Bryman, A. (2016). *Social research methods*. Oxford University Press.
- Bryman, A., & Bell, E. (2015). *Business research methods*. Oxford University Press.
- Buthelezi, M. P. (2017). *Addressing ambiguity within information security policies in higher education to improve compliance* [Master's dissertation, University of South Africa]. UNISA Institutional Repository. <http://hdl.handle.net/10500/23778>
- Carlsson, S., Henningsson, S., Hrastinski, S., & Keller, C. (2011). Socio-technical IS design science research: Developing design theory for IS integration management. *Information Systems and E-Business Management*, 9(1), 109–131.
- Chandarman, R., & Van Niekerk, B. (2017). Students' cyber security awareness at a private tertiary educational institution. *The African Journal of Information and*

*Communication*, 20, 133–155. <https://doi.org/10.23962/10539/23572>

City of Tshwane. (n.d.). *Welcome to free TshWi-Fi powered by the City of Tshwane*. <http://www.tshwane.gov.za/Pages/WIFI.aspx>

Cook, K. D. (2017). *Effective cyber security strategies for small businesses* [Doctoral dissertation, Walden University]. Walden University Repository. <https://scholarworks.waldenu.edu/dissertations/3871/>

Chi, M., Glaser, R., & Farr, M. (1988). *The Nature of Expertise*. Psychology Press.

Coertze, J. J. (2012). *A framework for information security governance in SMMEs* [Master's dissertation, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/d1014083>

Coetzer, C. (2015). *An investigation of ISO/IEC 27001 adoption in South Africa* [Master's dissertation, Rhodes University]. Rhodes Institutional Repository. <http://hdl.handle.net/10962/d1018669>

Crampton, N. (2019). *The definitive list of South African business incubators for start-ups*. Entrepreneur. <https://www.entrepreneur.com/article/327566>

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications.

Creswell, J. W., Clack, P., & Vicki, L. (2007). *Designing and conducting mixed methods research*. SAGE Publications.

Croasdell, D., Elste, J., & Hill, A. (2018). Cyber clinics: Re-imagining cyber security awareness. *Proceedings of the 51st Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/hicss.2018.538>

Cyber Resilience for Development. (n.d.). *We are Cyber 4 Dev*. <https://cyber4dev.eu/>

David, M., & Sutton, C. D. (2004). *Social research: The basics*. SAGE Publications.

- Deetz, S. (1996). Describing differences in approaches to organization science: Rethinking Burrell and Morgan and their legacy. *Organization Science*, 7(2), 191–207. <https://doi.org/10.1287/orsc.7.2.191>
- Department of Justice and Constitutional Development. (2017). *Cybercrimes and Cybersecurity Bill*. <https://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf>
- Devos, J., Landeghem, H., & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. *Industrial Management & Data Systems*, 112(2), 206–223. <https://doi.org/10.1108/02635571211204263>
- Dhillon, G., Stahl, B. C., & Baskerville, R. (2009). Creativity and intelligence in small and medium-sized enterprises: The role of information systems. *IFIP Advances in Information and Communication Technology*, 301, 1–9. [http://dx.doi.org/10.1007/978-3-642-02388-0\\_1](http://dx.doi.org/10.1007/978-3-642-02388-0_1)
- Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: A synergy approach. *7th International Conference on Information Warfare and Security, ICIW 2012*, 98–107. [https://doi.org/10.1007/978-3-8349-4134-3\\_3](https://doi.org/10.1007/978-3-8349-4134-3_3)
- Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. *Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW)*, 15–31.
- Dominguez, C. M. F., Ramaswamy, M., Martinez, E. M., & Cleal, M. (2010). A framework for information security awareness programs. *Issues in Information Systems*, 11(1), 402–409.
- Eisenhart, M. (1991). *Conceptual frameworks for research circa 1991: Ideas from a cultural anthropologist; implications for mathematics education rese.*
- Elgot, J., & Hern, A. (2018, March 19). *No 10 'very concerned' over Facebook data breach by Cambridge Analytica*. The Guardian. <https://www.theguardian.com/technology/2018/mar/19/no-10-very-concerned-over->

facebook-data-breach-by-cambridge-analytica

- Ellefsen, I. (2014). The development of a cyber security policy in developing regions and the impact on stakeholders. *2014 IST-Africa Conference Proceedings*, 1–10. <http://dx.doi.org/10.1109/ISTAFRICA.2014.6880605>.
- eNCA. (2020, September 16). *Credit bureau data breach probed*. <https://www.enca.com/business/credit-bureau-data-breach-probed>
- Ezzy, D. (2013). *Qualitative analysis*. Routledge.
- Fakeh, S. K. W., Zulhemay, M. N., Shahibi, M. S., Ali, J., & Zaini, M. K. (2012). Information security awareness amongst academic librarians. *Journal of Applied Sciences & Research*, 8(3), 1723-1735
- Fani, N., Von Solms, R., & Gerber, M. (2017). Governing information security within the context of bring your own device in SMMEs. *Institute of Electrical and Electronics Engineers Inc. (IEEE)*, 1-11. <https://doi.org/10.1109/ISTAFRICA.2016.7530586>
- Farooq, A. Isoaho, J. Virtanen, S., & Isoaho, J. (2015a). Information security awareness in educational institution: An analysis of students' individual factors. *IEEE Trustcom/BigDataSE/ISPA*, 352–359. <https://doi.org/10.1109/NCIA.2013.6725324>
- Farooq, A. Isoaho, J. Virtanen, S., & Isoaho, J. (2015b). Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy (IJISP)*, 9(2), 60–74. <http://doi.org/10.4018/IJISP.2015040104>
- Farooq, A., & Kakakhel, S. R. U. (2013). Information security awareness: Comparing perceptions and training preferences. *2nd National Conference on Information Assurance (NCIA)*, 53–57. <https://doi.org/10.1109/NCIA.2013.6725324>
- Fin24Tech. (2018, January 23). *Cyber risk biggest headache for SA business – report*. <https://www.fin24.com/Tech/News/cyber-risk-biggest-headache-for-sa-business->

- Fink, A. (2010). *Conducting research literature reviews: From the Internet to paper*. SAGE Publications.
- Fry, H., Ketteridge, S., & Marshallis, S. (2008). *A handbook for teaching and learning in higher education: Enhancing academic practice*. Routledge.
- Gcaza, N. (2017). *A national strategy towards cultivating a cybersecurity culture in South Africa* [Doctoral thesis, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/13735>
- Geerts, G. L. (2011). A design science research methodology and its application to accounting information systems research. *International journal of accounting Information Systems*, 12(2), 142–151.
- Ghazvini, A., & Shukur, Z. (2017). A framework for an effective information security awareness program in healthcare. *International journal of advanced computer science and applications*, 8(2), 193–205.
- Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead ... long live the paradigm: The legacy of Burrell and Morgan. *Omega*, 28(3), 249–268.
- Gregor, S., & Hevner, A. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337–355.
- Grobler, M., Van Vuuren, J., & Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. *ICT Critical Infrastructures and Society*, 215–225. [http://link.springer.com/chapter/10.1007/978-3-642-33332-3\\_20](http://link.springer.com/chapter/10.1007/978-3-642-33332-3_20)
- Grobler, M., Flowerday, S., Von Solms, R., & Venter, H. (2011a). Cyber awareness initiatives in South Africa: A national perspective. *Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW) 2011*, 32–41. <http://hdl.handle.net/10204/5164>



- Grobler, M., van Vuuren, J., & Zaaiman, J. (2011b). Evaluating cyber security awareness in South Africa. *Proceedings of the 10th European Conference on Information Warfare and Security. The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia*, 113-121. <http://hdl.handle.net/10204/5108>
- Guba, E. G. (1990). *The paradigm dialog*. SAGE Publications.
- Gundu, T., & Flowerday, S. V. (2013a). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, 104(2), 69–79.
- Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management and Computer Security*, 13(4), 297–310. <https://doi.org/10.1108/09685220510614425>
- Gunleifsen, H., Gkioulos, V., Wangen, A., Shalaginov, A., Kianpour, M., & Abomhara, M. (2019). Cyber security awareness and culture in rural Norway. *International Symposium on Human Aspects of Information Security & Assurance*. <http://hdl.handle.net/11250/2592269>
- Hassinen, T. (2017). *Enhancing Cyber Security for SME organizations through self-assessments: How self-assessment raises awareness* [Master's thesis, JAMK University of Applied Sciences]. JAMK Repository. <https://www.theseus.fi/handle/10024/125437>
- Harris, A. M., & Patten, P. K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97-114. <https://doi.org/10.1108/IMCS-03-2013-0019>
- Hassanzadeh, M., Jahangiri, N., & Brewster, B. (2013). A conceptual framework for information security awareness, assessment, and training. *Emerging trends in ICT security*. 99–110. Elsevier Inc. <https://doi.org/10.1016/B978-0-12-411474-6.00006-2>
- Hern, A. (2017, December 30). *WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017*. The Guardian. <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya->

ransomware

- Herselman, M., & Botha, A. (2015). Evaluating an artifact in design science research. *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists*, 1–10.
- Hevner, A., & Chatterjee, S. (2010). *Design science research in information systems*. Springer Science and Business Media.
- Hevner, A., March, S., & Park, J. (2004). Design science in information systems Research. *MIS Quarterly*, 28(1), 75–105.
- Hofstee, E. (2006). *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule*. EPE.
- Holbrook, A. L., Krosnick, J. A., Moore, D., & Tourangeau, R. (2007). Response order effects in dichotomous categorical questions presented orally: The impact of question and respondent attributes. *Public Opinion Quarterly*, 71(3), 325–348.
- Holdsworth, J., & Apeh, E. (2017). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. *Proceedings - 2017 IEEE 25th International Requirements Engineering Conference Workshops, REW 2017*, 111–117. <https://doi.org/10.1109/REW.2017.47>
- Holland, P. (2017, February 25). *Cloudbleed bug: Everything you need to know*. CNET. <https://www.cnet.com/how-to/cloudbleed-bug-everything-you-need-to-know/>
- Hubbard, J. (2019, March 13). *SA business underplaying the danger of cybercrime?* Fin24Tech. <https://www.fin24.com/Finweek/Business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313>
- Introna, L. D. (2011). Hermeneutics and meaning-making in information systems. *The Oxford Handbook of Management Information Systems: Critical Perspectives and New Directions*, 229–252. <https://doi.org/https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/97801995>

- IRMSA. (2017). *IRMSA risk report South Africa risks 2017 Third Edition*. [https://cdn.ymaws.com/www.irmsa.org.za/resource/resmgr/website\\_imagery/irmsa\\_risk\\_report\\_2017\\_-\\_fin.pdf](https://cdn.ymaws.com/www.irmsa.org.za/resource/resmgr/website_imagery/irmsa_risk_report_2017_-_fin.pdf)
- ISO/IEC 27000. (2009). *ISO/IEC 27000: Information technology — security techniques — information security management systems — overview and vocabulary*.
- Jansen, H., & Hak, T. (2005). The productivity of the three-step test interview (TSTI) compared to an expert review of a self-administered questionnaire on alcohol consumption. *Journal of Official Statistics: An International Quarterly*, 21(1), 103–120.
- Jordaan, P. (2014). *Information security awareness in small information technology-dependent business organisations* [Master's dissertation, University of Johannesburg]. UJ Institutional Repository. <http://hdl.handle.net/10210/13566>
- Jugder, N. (2016). The thematic analysis of interview data: An approach used to examine the influence of the market on curricular provision in Mongolian higher education institutions. *University of Leeds*. <https://hpp.education.leeds.ac.uk/wp-content/uploads/sites/131/2016/02/HPP2016-3-Jugder.pdf>
- Kajornboon, A. B. (2005). Using interviews as research instruments. *E-Journal for Research Teachers*, 2(1), 1–9.
- Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *International Conference on Research and Innovation in Information Systems*, 286–290. <https://doi.org/10.1109/ICRIIS.2013.6716723>
- Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: The case of web server logs and intrusion detection. *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 100–105.

- Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers and Security, 70*, 663–674. <https://doi.org/10.1016/j.cose.2017.08.001>
- Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115–126. <https://doi.org/10.1108/IMCS-01-2013-0005>
- Koornhof, H. (2009). *A framework for IT governance in small businesses* [Master's dissertation, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/994>
- Kortjan, N. (2013). *A cyber security awareness and education framework for South Africa* [Master's dissertation, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/d1014829>
- Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal, 52*. <https://doi.org/10.18489/sacj.v52i0.201>
- Kritzinger, E. (2006). *An information security retrieval and awareness model for industry* [Doctoral thesis, University of South Africa]. UNISA Institutional Repository. <http://hdl.handle.net/10500/4006>
- Kritzinger, E., Bada, M., & Nurse, J. R. C. (2017). A study into the cyber security awareness initiatives for school learners in South Africa and the UK. *IFIP World Conference on Information Security Education*, 110–120.
- Kritzinger, E., Loock, M., & Mwim, E. (2018). Cyber safety awareness and culture planning in South Africa. *International Symposium on Cyberspace Safety and Security*, 317–326. [https://link.springer.com/chapter/10.1007/978-3-030-01689-0\\_25](https://link.springer.com/chapter/10.1007/978-3-030-01689-0_25)
- Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security, 27*(5–6), 224–231. <https://doi.org/10.1016/j.cose.2008.05.006>

- Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, 29(8), 840–847. <https://doi.org/10.1016/j.cose.2010.08.001>
- Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*, 1-7. <https://doi.org/10.1109/ISSA.2011.6027505>
- Kruger, H. A., Drevin, L., & Steyn, T. (2006). A framework for evaluating ICT security awareness. *Proceedings of the ISSA 2006 Conference*, 1–11. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.7113&rep=rep1&type=pdf>
- Kruger, H. A., Drevin, L., & Steyn, T. (2010). The use of an information security vocabulary test to assess information security awareness – An exploratory study. *Proceedings of the South African Information Security Multi-Conference, SAISMC 2010*, 13–22. <http://hdl.handle.net/10394/19404>
- Kruger, H., Drevin, L., & Steyn, T. (2010b). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5). <https://doi.org/10.1108/09685221011095236>
- Labuschagne, W., Veerasamy, N., Leenen, L., & Mujinga, M. (2011a). Design of a cyber security awareness campaign for internet café users in rural areas. *Southern African Cyber Security Awareness Workshop (SACSAW)*, 42-58. <http://hdl.handle.net/10204/5165>
- Labuschagne, W. A., Burke, I., Veerasamy, N., & Eloff, M. M. (2011b). Design of cyber security awareness game utilizing a social media framework. *2011 Information Security for South Africa – Proceedings of the ISSA 2011 Conference*, 1-9. <https://doi.org/10.1109/ISSA.2011.6027538>
- Labuschagne, W. A., Veerasamy, N., Leenen, L., & Mujinga, M. (2011c). Damp internet

café users in rural design of a cyber security awareness campaign for internet café users in rural areas. *Proceedings of Southern African Cyber Security Awareness Workshop*, 42–58.

Lame, G. (2019). Systematic literature reviews: An introduction. *Proceedings of the Design Society: International Conference on Engineering Design*, 1(1), 1633–1642. doi:10.1017/dsi.2019.169

Larson, S. (2017, October 4). *Every single Yahoo account was hacked - 3 billion in all*. CNN. <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html>

Laverty, S. M. (2003). Hermeneutic phenomenology and phenomenology: A comparison of historical and methodological considerations. *International Journal of Qualitative Methods*, 2(3), 21-35. <https://doi.org/10.1177%2F160940690300200303>

Le Roux, F. (2010). *The applicability of the Third King Report on corporate governance to small and medium enterprises* [Master's dissertation, Stellenbosch University]. Stellenbosch University Institutional Repository. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.928.7589&rep=rep1&type=pdf>

Leary, M. (2016). *Introduction to behavioral research methods*. Pearson Education.

Leedy, P., & Ormrod, J. (2001). *Practical research: Planning and design*. Merrill Prentice-Hall.

LeFebvre, R. (2012). The human element in cyber security: a study on student motivation to act. *Proceedings of the 2012 Information Security Curriculum Development Conference*, 1–8. <https://doi.org/10.1145/2390317.2390318>

Lejaka, T. K., Da Veiga, A., & Loock, M. (2019). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. *2019 Conference on Information Communications Technology and Society, ICTAS 2019*, 1-6. <https://doi.org/10.1109/ICTAS.2019.8703609>

- Lewis, V. L., & Churchill, N. C. (1983). The five stages of small business growth. *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship*.
- Li, J., Wang, Y., & Qi, B. (2018). Discussion on cyber security awareness and awareness model building based on connectionism. *Proceedings of 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference, ITOEC 2018*, 259-263. <https://doi.org/10.1109/ITOEC.2018.8740446>
- Lupiana, D. (2008). *Development of a framework to leverage knowledge management systems to improve security awareness* [Master's dissertation, Dublin Institute of Technology]. Dublin Institute of Technology Repository. <https://arrow.tudublin.ie/scschcomdis/6/>
- Maclellan, E. & Soden, R. (2003). Expertise, expert teaching and experienced teachers' knowledge of learning theory. *Scottish Educational Review*, 35(2), 110–120.
- Mahadea, D., & Pillay, M. K. (2008). Environmental conditions for SMME development in a South African province. *South African Journal of Economics and Management Sciences*, 11(4), 431–448.
- Makhudu, A. B., Mavetera, N., & Mavetera, C. (2012). Investigating information system security policy and awareness training programs in South African organizations. *Innovation Vision 2020: Sustainable Growth, Entrepreneurship, and Economic Development - Proceedings of the 19th International Business Information Management Association Conference*, 4, 1870–1882.
- March, S., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15, 251–266.
- McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M. & Lillie, M. (2018), The effect of resilience and job stress on information security awareness, *Information and Computer Security*, 26(3), 277–289. <https://doi.org/10.1108/ICS-03-2018-0032>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017).

Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>

Meggison, L., Byrd, M., & Meggison, W. (2006). *Small business management: An entrepreneur's guidebook*. McGraw-Hill Higher Education.

Meyer, I. A. (2017). *A framework for decision-making in ICT4D interventions to enable sustained benefit in resource-constrained environments* [Doctoral thesis, University of South Africa]. UNISA Institutional Repository. <http://hdl.handle.net/10500/23834>

Moallem, A. (2019). Cyber security awareness among college students. *Advances in Intelligent Systems and Computing*, 79-87. [https://doi.org/10.1007/978-3-319-94782-2\\_8](https://doi.org/10.1007/978-3-319-94782-2_8)

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, 6(7). <https://doi.org/doi:10.1371/journal.pmed.1000097>

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education : An exploratory study. *2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings*, 1-6. <https://doi.org/10.1109/ICTAS47918.2020.233978>

Morgan, A., Colebourne, D., & Thomas, B. (2006). The development of ICT advisors for SME businesses: An innovative approach. *Technovation*, 26(8), 980–987. <https://doi.org/10.1016/j.technovation.2005.09.001>

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, 1(2), 13–22.

Moyo, A. (2021, June 02). *President Ramaphosa signs Cyber Crimes Bill into law*. ITWeb. <https://www.itweb.co.za/content/LPp6VMrDJJovDKQz>

Myers, M. D. (2013). *Qualitative research in business & management*. SAGE



Publications.

Myers, M. D., & Avison, D. (2002). *Qualitative research in information systems*. SAGE Publications.

National Planning Commission. (2011). *National Development Plan: Vision for 2030*. [https://www.gov.za/sites/default/files/gcis\\_document/201409/devplan2.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/devplan2.pdf)

National Research Council. (2000). *How people learn: Brain, mind, experience, and school: Expanded edition*. National Academies Press.

Newman, L. H. (2017, February 24). Massive bug may have leaked user data from millions of sites. So ... change your passwords. *Wired*. <https://www.wired.com/2017/02/crazy-cloudflare-bug-jeopardized-millions-sites/>

News24 Wire. (2016, March 02). *Inside SIM-swap job at FNB and MTN scammed customers: Investigator*. MyBroadband. <https://mybroadband.co.za/news/cellular/157239-inside-sim-swap-job-at-fnb-and-mtn-scammed-customers-investigator.html>

Ngalonkulu, M. (2018, November 04). Small businesses a gateway to bigger companies for hackers. *The Citizen*. <https://citizen.co.za/business/business-small-business/2199869/small-businesses-a-gateway-to-bigger-companies-for-hackers/>

Ngoqo, B., & Flowerday, S. V. (2014). Linking student information security awareness and behavioural intent. *Proceedings of the 8th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2014*, 162–173.

Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information and Computer Security*, 23(4), 406–420. <https://doi.org/10.1108/ics-10-2014-0072>

Nichter, S., & Goldmark, L. (2009). Small firm growth in developing countries. *World Development*, 37(9), 1453–1464.

- Niehaves, B. (2007). On epistemological diversity in design science – new vistas for a design-oriented IS research? *International Conference on Information Systems*, 28(133). <https://aisel.aisnet.org/icis2007/133/>
- Nieman, G., & Nieuwenhuizen, C. (2014). *Entrepreneurship: A South African perspective*. Van Schaik.
- Oates, B. J. (2006). *Researching information systems and computing*. SAGE Publications.
- OECD. (2015). *OECD Economic surveys South Africa July 2015 overview*. <http://www.oecd.org/eo/surveys/South-Africa-OECD-economic-survey-overview.pdf>
- Okesola, J. O., & Grobler, M. (2014). Developing a secured social networking site using information security awareness techniques. *SA Journal of Information Management*, 16(1). <https://doi.org/10.4102/sajim.v16i1.607>
- Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems*, 10(26), 1–49.
- Ouma, S. (2013). *M-health user experience framework for the public healthcare sector* [Doctoral thesis, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/d1020793>
- Park, J. Y., Robles, R. J., Hong, C. H., Yeo, S. S., & Kim, T. H. (2008). IT security strategies for SME's. *International Journal of Software Engineering and Its Applications*, 2(3), 91–98.
- Partington, D. (2002). *Essential skills for management research*. SAGE Publications.
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2014), A study of information security awareness in Australian government organisations, *Information Management & Computer Security*, 22(4), 334–345. <https://doi.org/10.1108/IMCS-10-2013-0078>

- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information and Computer Security*, 25(2), 181–189. <https://doi.org/10.1108/ICS-03-2017-0017>
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–78.
- Pfleeger, C., & Pfleeger, S. (2006). *Security in computing*. Prentice-Hall.
- Popular Mechanics. (2017). *Cloudbleed explained: Protect yourself from the internet's new security flaw*.  
<https://www.popularmechanics.com/technology/security/a25380/cloudbleed-explained/>
- Potgieter M., Marais C., & Gerber M. (2013). Fostering content relevant information security awareness through browser extensions. *IFIP World Conference on Information Security Education. Information Assurance and Security Education and Training*, 406, 58–67. [https://doi.org/10.1007/978-3-642-39377-8\\_7](https://doi.org/10.1007/978-3-642-39377-8_7)
- Purao, S. (2002). Design research in the technology of information systems: Truth or dare. *GSU Department of CIS Working Paper*, 45–77.
- PwC. (2016). Economic crime: A South African pandemic. No sector or region is immune. *Global Economic Crime Survey 2016. 5th South African Edition. March 2016*.  
<https://www.pwc.co.za/en/assets/pdf/south-african-crime-survey-2016.pdf>
- PwC. (2020). Economic crime: When the boardroom becomes the battlefield. *Global Economic Crime and Fraud Survey 2020. 7th South African Edition. March 2020*.  
<https://www.pwc.co.za/en/assets/pdf/global-economic-crime-survey-2020.pdf>
- Rees, J. (2010). Information security for small and medium-sized business. *Computer Fraud & Security*, 9, 18–19. [https://doi.org/10.1016/S1361-3723\(10\)70123-8](https://doi.org/10.1016/S1361-3723(10)70123-8)

- Reid, R. (2017). *Guidelines for cybersecurity education campaigns* [Doctoral thesis, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/14091>
- Rossi, M., & Sein, M. K. (2003). Design research workshop: A proactive research approach. *IRIS*, 26, 9–112.
- Rastogi, R., & Von Solms, R. (2012). Information security service branding - Beyond information security awareness. *Systemics, Cybernetics and Informatics*, 10(3), 54–159.
- SAASTA. (n.d.). *Overview*. <https://www.saasta.ac.za/about-us/overview/>
- Sami, W. (2016). *Exploring the strategising practices of small business managers in selected small businesses in the accommodation sector in Tshwane metropolitan area* [Master's dissertation, University of South Africa]. UNISA Institutional Repository. <http://hdl.handle.net/10500/22203>
- Sánchez, L., Ruiz, C., Fernández-Medina, E., & Piattini, M. (2010). Managing the asset risk of SMEs. *International Conference on Availability, Reliability and Security*, 60, 422–429. <https://doi.org/10.1109/ARES.2010.52>
- Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students*. Pearson Education.
- Scarborough, N., & Zimmerer, T. W. (2006). *Effective small business management: An entrepreneurial approach*. Pearson Education.
- Shabe, T., Kritzinger, E., & Looock, M. (2017). Scorecard approach for cyber-security awareness. *International Symposium on Emerging Technologies for Education*, 144–153.
- Sherr, I. (2017, May 19). *WannaCry ransomware: Everything you need to know*. CNET. <https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/>

- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41. <https://doi.org/10.1108/09685220010371394>
- Small Enterprise Development Agency. (n.d.). *About us*. <http://www.seda.org.za/AboutUs/Pages/Home.aspx>
- Small Enterprise Development Agency. (2019). *SMME quarterly update 1st quarter 2019*. <http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%202019-Q1.pdf>
- 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>
- Solon, O., & Hern, A. (2017, June 28). ‘Petya’ ransomware attack: What is it and how can it be stopped? *The Guardian*. <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>
- Soni, P., Cowden, R., & Karodia, A. M. (2015). Investigating the characteristics and challenges of SMMEs in the Ethekewini Metropolitan Municipality. *Nigerian Chapter of Arabian Journal of Business and Management Review*, 3(10), 15–93. <https://doi.org/10.12816/0017683>
- South Africa. (2004). *National Small Business Amendment Act 29 of 2004*. [https://www.gov.za/sites/default/files/gcis\\_document/201409/a29-04.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/a29-04.pdf)
- South African Institute of Chartered Accountants. (2015). *2015 SME insights report*. [https://www.saica.co.za/portals/0/documents/saica\\_sme.pdf](https://www.saica.co.za/portals/0/documents/saica_sme.pdf)
- Spiegelhalter, K. (2014). *Research design and ethics: Intersections in innovation-mindfulness, therapies, behavioural economics and marginalised groups*. SAGE Publications.

- Staff Writer. (2017, September 03). *R1.6 million stolen from ABSA client after Vodacom SIM-swap fraud*. MyBroadband. <https://mybroadband.co.za/news/security/227503-r1-6-million-stolen-from-absa-client-after-vodacom-sim-swap-fraud.html>
- Stephanou, A. (2008). *The impact of information security awareness training on information security behavior* [Master's dissertation, University of the Witwatersrand]. Wits Institutional Repository. <http://hdl.handle.net/10539/7421>
- Stewart, G. & Lacey, D. (2012), Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1), 29–38. <https://doi.org/10.1108/09685221211219182>
- Stokes, D., & Wilson, N. (2010). *Small business management and entrepreneurship*. Cengage Learning (EMEA).
- Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *African Journal of Information and Communication (AJIC)*, 20, 83–112. <https://doi.org/10.23962/10539/23574>
- Swanborn, P. (2010). *Case study research: What, why and how?* SAGE Publications.
- Symantec. (2017). *Internet security threat report, Vol. 22. April 2017*. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>
- Symantec. (2019). *Internet security threat report, Vol. 24. February 2019*. <https://docs.broadcom.com/doc/istr-24-2019-en>
- Tariq, M. A., Brynielsson, J., & Artman, H. (2014). The security awareness paradox: A case study. *ASONAM 2014 - Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 704–711. <https://doi.org/10.1109/ASONAM.2014.6921663>
- Thomas, E., & Magilvy, J. K. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing*, 16(2), 151-155. <https://doi.org/10.1111/j.1744-6155.2011.00283.x>

- Tirumala, S. S., Valluri, M. R., & Babu, G. (2019). A survey on cyber security awareness concerns, practices and conceptual measures. *International Conference on Computer Communication and Informatics*, 1-6. <https://doi.org/10.1109/iccci.2019.8821951>
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, 25(3), 327–352. [https://www.researchgate.net/publication/233808205\\_Analyzing\\_Trajectories\\_of\\_Information\\_Security\\_Awareness](https://www.researchgate.net/publication/233808205_Analyzing_Trajectories_of_Information_Security_Awareness)
- Upfold, C. T. (2005). *An investigation of information security in small and medium enterprises (SMEs) in the Eastern Cape* [Master's dissertation, Rhodes University]. Rhodes Institutional Repository. <http://hdl.handle.net/10962/d1003847>
- Upfold, C. T., & Sewry, D. A. (2005). An investigation of information security In small and medium enterprises (SME's) in the Eastern Cape. *Proceedings of the ISSA 2005 New Knowledge Today Conference*. [http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082\\_Article.pdf](http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf)
- USAToday. (2017, November 08). *Marissa Mayer says Yahoo still doesn't know who was behind Web's biggest breach*. <https://www.usatoday.com/story/tech/news/2017/11/08/marissa-mayer-says-yahoo-still-doesnt-know-who-behind-webs-biggest-breach/844716001/>
- Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems. <http://desrist.org/design-research-in-information-systems/>
- Van de Haar, P. (2014). *Towards a wireless local area network security control framework for small, medium and micro enterprises in South Africa* [Master's dissertation, Nelson Mandela University]. NMU Institutional Repository. <http://hdl.handle.net/10948/4001>
- Van Zyl, G. (2016, March 02). *Thousands of rands lost in 'FNB, MTN scam'*. Fin24Tech. <https://www.fin24.com/Tech/Mobile/thousands-of-rands-lost-in-fnb-mtn-scam-20160302>
- Van Zyl, I. (2015). *Disciplinary kingdoms: Navigating the politics of research philosophy*

in the information systems. *Electronic Journal of Information Systems in Developing Countries*, 70(1), 1–17.

Venktesh, K. (2017, October 19). *Dead or alive: SA data leak tallies 60 million ID numbers*. Fin24Tech. <https://www.fin24.com/Tech/Cyber-Security/dead-or-alive-sa-data-leak-tallies-60-million-id-numbers-20171019>

Vermeulen, J. (2017, March 09). *Massive flaw in old Ster-Kinekor website leaked clients' private data*. MyBroadband. <https://mybroadband.co.za/news/security/202208-massive-flaw-in-old-ster-kinekor-website-leaked-clients-private-data.html>

Von Solms, B. (2015). Improving South Africa's cyber security by cyber securing its small companies. *2015 IST-Africa Conference, IST-Africa 2015*, 1-8. <https://doi.org/10.1109/ISTAFRICA.2015.7190538>

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2–9. <https://doi.org/10.1108/ICS-04-2017-0025>

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>

Walaza, M., Loock, M., & Kritzinger, E. (2014). A framework to integrate ICT security awareness into the South African schooling system. *ACM International Conference Proceeding Series*, 11–18. <https://doi.org/10.1145/2664591.2664596>

Walaza, M., Loock, M., & Kritzinger, E. (2020). A framework to enhance ICT security through education, training and awareness (ETA) programmes in South African small, medium and micro-sized enterprises (SMMEs): A scoping review. *Advances in Intelligent Systems and Computing*, 45-58. [https://doi.org/10.1007/978-3-030-51974-2\\_5](https://doi.org/10.1007/978-3-030-51974-2_5)

Wang, Y., Qi, B., Zou, H. X., & Li, J. X. (2019). Framework of raising cyber security awareness. *International Conference on Communication Technology Proceedings, ICCT*, 865-869. <https://doi.org/10.1109/ICCT.2018.8599967>



Welman, J. C., & Kruger, S. J. (2001). *Research methodology*. Oxford University Press.

World Economic Forum. (2017). *The African competitiveness report 2017*.  
[http://www3.weforum.org/docs/WEF\\_ACR\\_2017.pdf](http://www3.weforum.org/docs/WEF_ACR_2017.pdf)

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, 39(1), 93–112.

Yunos, Z., Hamid, R. S. A., & Ahmad, M. (2016). Development of a cyber security awareness strategy using focus group discussion. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1063–1067.  
<https://doi.org/10.1109/SAI.2016.7556109>

## 8 LIST OF APPENDICES

### 8.1 APPENDIX A: TABLES

Appendix 8-1: Studies which met the inclusion criteria for security awareness in South Africa

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMES	Included in study
1. "A conceptual framework for cyber-security awareness and education in SA"	Kortjan & von Solms (2014)	Qualitative	Journal article	"Proposes a cyber-security awareness and education framework for SA that would assist in creating a cyber-secure culture in SA among all of the users of the internet."				×	×	×
2. "Ignorance to awareness: Towards an information security awareness process"	Gundu & Flowerday (2013a)	Quantitative	Journal article	"This paper presents an information security awareness process that seeks to cultivate positive security behaviours using a behavioural intention model based on the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory."	×		×		×	×
3. "The enemy within: A behavioural intention model and an information security awareness process"	Gundu & Flowerday (2013b) ( <i>Same research concept as 2013a</i> )	Qualitative	Conference paper	"This paper presents an information security awareness process that seeks to cultivate positive security behaviours using the behavioural intentions models."	×		×		×	×

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
4. "Improving South Africa's Cyber Security by cyber securing its small companies"	Von Solms (2015)	Qualitative	Conference paper	"This paper is therefore to create a Plan of Action to be initiated by the SA Government to provide help and support to small companies in SA to improve their levels of cyber security."		✗			✗	✗
5. "The development of a cyber security policy in developing regions and the impact on stakeholders"	Ellefsen (2014)	Qualitative	Conference paper	"This paper outlines and discusses the developing cyber security policy framework in South Africa and the implications on SMMEs as a component of the resulting protection structures."					✗	
6. "How South African SMEs address cyber security: The case of web server logs and intrusion detection"	Kent et al. (2016)	Qualitative	Conference paper	"The purpose is to investigate the factors that influence SMEs cyber security implementations."					✗	
7. "Creating a Cyber Skills Framework for South Africa"	Phillips (n.d.)	Qualitative		"In this paper, we set out to argue the case for a cybersecurity curriculum for South Africa and identified distinct users of cyberspace in South Africa and the skills training they require in order to safely navigate across cyberspace."				✗		
8. "Parliamentary oversight of Cyber Security and Critical	Von Solms (2013)	Qualitative	Conference paper	"This paper investigates the role of Parliamentary oversight over the Cyber Security health and Critical Information Infrastructure Protection		✗				

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
Information Infrastructures in Developing Countries”				(CIIP) of a country, with special reference to Developing Countries.”						
9. “Information security awareness in small information technology-dependent business organisations”	Jordaan (2014)	Qualitative	Masters Dissertation	“This research study identifies the level of information security awareness espoused in small IT dependant businesses around the Gauteng province of South Africa.”	×				×	×
10. “Enhancing information security education and awareness: Proposed characteristics for a model”	Amankwa, Loock, & Kritzinger (2016)	Qualitative	Conference paper	“This paper categorized models for enhancing security education and awareness based on their stakeholder domains into: End-Users, Institutions and Industry domains.”		×				×
11. “Framework for an African policy towards creating cyber security awareness”	Dlamini et al. (2011)	Qualitative	Conference paper	“This paper proposes a high-level African Cyber Security Policy as well as an African Cyber Security Awareness Framework to guide cyber security agencies, standards and legislation as well as specific initiatives to promote cyber security awareness.”				×	×	×
12. “A cyber security awareness and education framework for South Africa”	Kortjan (2013)	Qualitative	Masters Dissertation	“This research proposes a cyber security awareness and education framework for SA that will assist in creating a cyber secure culture in SA among all of its users of the internet.”				×	×	×

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
13. "An investigation of information security in small and medium enterprises (SME's) in the Eastern Cape"	Upfold (2005)	Quantitative	Masters Dissertation	"Investigate information security, especially with regard to Small and Medium enterprises (SME's)."					X	
14. "Governance of cybersecurity—the case of South Africa"	Sutherland (2017)	Qualitative	Journal article	"This article considers the governance of cybersecurity in South Africa, a complex federal state with a relatively sophisticated economy, though with many impoverished citizens who often have limited digital literacy."		X				
15. "Architecture for managing knowledge on cybersecurity in Sub-Saharan Africa"	Andoh-Baidoo et al. (2014)	Qualitative	Journal paper	"This paper presents an architecture for managing knowledge on cybersecurity in Sub-Saharan Africa. The architecture enables the creation and exchange of knowledge on cybersecurity especially for home users while providing awareness and enforcement mechanisms to help home users protect themselves against cyber threat."					X	
16. "The impact of information security awareness training on information security behavior"	Stephanou (2008)	Quantitative	Masters Dissertation	"This research aims to answer the question: To what extent does information security awareness training influence information security behaviour?"		X				

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
17. "An information security retrieval and awareness model for industry"	Kritzinger (2006)	Qualitative	PhD Thesis	"This study proposes the ISRA model for industry that ensures that stakeholders are made aware of the Information Security issues relevant to their specific job category only, to prevent them from being burdened with irrelevant information."			X			X
18. "Effective Cyber Security Strategies for Small Businesses"	Cook (2017)	Qualitative	PhD Thesis	"This study explores the strategies among owners of 4 retail SMEs who successfully protected their businesses against cyber attacks."		X			X	
19. "Guidelines for cybersecurity education campaigns"	Reid (2017)	Mixed	PhD Thesis	"This thesis addressed the lack of guidance for designing and implementing cybersecurity and cybersafety educational campaigns suited to school learners as a target audience."		X				
20. "The Human Element in Cyber Security: A Study on Student Motivation to Act"	LeFebvre (2012)	Quantitative	Conference paper	"This study examines how general student are motivated to protect themselves from the threat of cybercrime."	X					
21. "Improving Security Awareness in the Government Sector"	Amjad, Naeem, Zaffar, Zaffar, & Choo (2016)	Quantitative	Conference paper	"This study helps to understand the level of cyber security awareness and understanding in the Government sector."	X					
22. "The Urgent Need for an Enforced Awareness"	Adelola et al. (2015)	Qualitative	Conference paper	"This study establishes the need for an enforced Internet security awareness programme for Nigeria that would assist in creating a cyber-	X					

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
Programme to Create internet Security Awareness in Nigeria”				secure culture in Nigeria among all of the users of the internet.”						
23. “Analyzing trajectories of information security awareness”	Tsohou, Karyda, Kokolakis, & Kiountouzis (2012)	Qualitative	Journal article	“The purpose of the paper is to increase understanding why security awareness programs are not working as they should. The study illuminate the problems that organizations face when trying to establish an information security awareness program.”		X				
24. “A vocabulary test to assess information security awareness”	Kruger et al (2010b)	Quantitative	Journal article	“The purpose of this paper is to examine the feasibility of an information security vocabulary test as an aid to assess awareness levels and to assist with the identification of suitable areas or topics to be included in an information security awareness program.”	X					X
25. “The use of an information security vocabulary test to assess information security awareness - An exploratory study”	Kruger et al. (2010) (the same research concept)	Quantitative	Conference paper	“The aim of this paper is to examine the feasibility of an information security vocabulary test as an aid to assess awareness levels and to help with the identification of suitable areas or topics to be included in an information security awareness program.”	X					
26. “A systematic review of approaches to	Rahim et al. (2015)	Qualitative	Journal article	“The purpose of this paper is to survey, explore and inform researchers about the previous		X				

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
assessing cybersecurity awareness”				methodologies applied, target audience and coverage of previous assessment of cyber security awareness by capturing, summarizing, synthesizing and critically comment on it.”						
27. “Recommendations for information security awareness training for college students”	Kim (2014)	Quantitative	Journal article	“The purpose of this paper is to survey the status of information security awareness among college students in order to develop effective information security awareness training (ISAT).”	X					
28. “A study of information security awareness in Australian government organisations”	Parsons, McCormac, Pattinson, Butavicius, & Jerram (2014)	Quantitative	Journal article	“The purpose of this paper is to investigate the human-based information security vulnerabilities in three Australian government organisations.”	X					
29. “Managing information security awareness at an Australian bank: a comparative study”	Pattinson et al. (2017)	Quantitative	Journal article	“The aim of this study was first to confirm that a specific bank’s employees were generally more information security-aware than employees in other Australian industries and second to identify the major factors that contributed to this bank’s high levels of ISA.”	X					
30. “The effect of resilience and job stress on information security awareness”	McCormac, Calic, Parsons, Butavicius,	Quantitative	Journal article	“The purpose of this study was to investigate the relationship between resilience, job stress and information security awareness (ISA).”	X					



Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
	Pattinson, & Lillie (2018)									
31. "Exploring the relationship between student mobile information security awareness and behavioural intent"	Ngoqo & Flowerday (2015)	Quantitative	Journal article	"This research paper explores the relationship between student mobile phone user information security awareness and behavioural intent in a developmental university in South Africa."	X					X
32. "Death by a thousand facts: Criticising the technocratic approach to information security awareness"	Stewart & Lacey (2012)	Qualitative	Journal article	"The purpose of this paper is to examine why mainstream information security awareness techniques have failed to evolve at the same rate as automated technical security controls and to suggest improvements based on psychology and safety science."		X				
33. "The effects of the PoPI Act on small and medium enterprises in South Africa"	Botha, Eloff, & Swart (2015)	Quantitative	Conference paper	"This paper explores the possible effects of the PoPI Act on SMEs in South Africa, focusing in particular on the marketing strategies used by surveyed SMEs."					X	
34. "Students' cybersecurity awareness at a private tertiary educational institution"	Chandarman & van Niekerk (2017)	Quantitative	Journal article	"This article measures the levels of CSA among students at a private tertiary education institution in South Africa."	X					X

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
35. "Developing a secured social networking site using information security awareness techniques"	Okesola & Grobler (2014)	Qualitative	Journal article	"This article presented sOcialistOnline – a newly developed SNS, duly secured and platform independent with various ISA techniques fully implemented."			X			
36. "Persona-centred information security awareness"	Ki-Aries & Faily (2017)	Qualitative	Journal article	"This paper presents an approach for identifying security related human factors by incorporating personas into information security awareness design and implementation."	X					
37. "Smartphone information security awareness: A victim of operational pressures"	Allam et al. (2014)	Qualitative	Journal article	"This paper explores the factors which influence these oscillating levels of information security awareness."			X			X
38. "Enhancing cyber security awareness with mobile games"	Alotaibi et al. (2017)	Quantitative	Conference paper	"The study aims to address the issue of creating cybersecurity awareness by employing gameplay methods over traditional approaches to make awareness process more engaging."	X					
39. "A survey of cyber-security awareness in Saudi Arabia"	Alotaibi, Furnelli, et al (2016)	Quantitative	Conference paper	"This paper investigates the cyber security awareness of the people in Saudi Arabia within different contexts."	X					
40. "Scorecard approach for cyber-security awareness"	Shabe et al. (2017)	Quantitative	Conference paper	"The study used a scorecard approach to measure the level of cyber-security awareness"	X					X

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
				among cell phone users in Rocklands Township, South Africa.”						
41. “A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK”	Kritzinger et al. (2017)	Qualitative	Conference paper	“This research reports on a study into the cybersecurity awareness initiatives for school learners in South Africa and the UK, which are supported by government, industry and academia.”		X				X
42. “Information security awareness in educational institution: An analysis of students' individual factors”	Farooq, Isoaho, Virtanen, & Isoaho (2015a)	Quantitative	Conference paper	“The purpose of this paper is to study information security awareness (ISA) among university students and further analyze how different individual factors impact it.”	X					
43. “Observations on genderwise differences among university students in information security awareness”	Farooq, Isoaho, Virtanen, & Isoaho (2015b)	Quantitative	Journal paper	“The purpose of this study is to examine genderwise differences in information security awareness (ISA) among university students.”	X					
44. “Linking student information security awareness and behavioural intent”	Ngoqo & Flowerday (2014)	Quantitative	Conference paper	“This paper explores the relationship between student mobile phone user information security awareness and behavioural intent in a developmental university in South Africa.”	X					X

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
45. "A conceptual analysis of information security education, information security training and information security awareness definitions"	Amarkwa, Loock, & Kritzinger (2014)	Qualitative	Conference paper	"This paper presents working definitions for information security education, information security training and information security awareness."		X				X
46. "Fostering content relevant information security awareness through browser extensions"	Potgieter et al. (2013)	Qualitative	Conference paper	"This study suggests using browser integration as a medium to promote security values and provide security suggestions based on a specific users behavioural pattern."			X			X
47. "Information security awareness: Comparing perceptions and training preferences"	Farooq & Kakakhel (2013)	Quantitative	Conference paper	"This study is carried out to compare and understand the perceived Information Technology (IT) and Information Security knowledge level of Information and Communication Technologies (ICT) users of two countries, Pakistan and Finland."	X					
48. "Information security awareness amongst academic librarians"	Fakeh et al. (2012)	Quantitative	Journal article	"This study seeks the level of awareness amongst academic librarians in private colleges in the districts of Shah Alam, Petaling Jaya, and Damansara."	X					

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
49. "Cyber security awareness initiatives in South Africa: A synergy approach"	Dlamini & Modise (2012)	Qualitative	Conference paper	"This paper evaluates the extent to which the current cyber security awareness initiatives address the cyber security threats and risks."		×				×
50. "Evaluating cyber security awareness in South Africa"	Grobler, Van Vuuren, & Zaaiman (2011b)	Quantitative	Conference paper	"This paper discusses the preparation, evaluation and training of South African rural communities with regard to cyber security awareness."		×				×
51. "Design of cyber security awareness game utilizing a social media framework"	Labuschagne et al. (2011b)	Qualitative	Conference paper	"This paper proposes an interactive game hosted by social networking sites with the purpose of creating awareness on information security threats and vulnerabilities."			×			×
52. "An assessment of the role of cultural factors in information security awareness"	Kruger et al. (2011)	Quantitative	Conference paper	"The objective is to determine whether cultural differences among students have an effect on their ICT security awareness levels."	×					×
53. "Information security service branding - Beyond information security awareness"	Rastogi & Von Solms (2012)	Qualitative	Journal article	"This paper borrows the concepts of branding from marketing to describe the process for creating the information security service brand in the organisation to counter negative image of information security."		×				

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
54. "Five Dimensions of Information Security Awareness"	Siponen (2000)	Qualitative	Journal article	"This paper outlines the dimensions of information security awareness, namely its organizational, gene~ public, socio-political, computer ethical and institutional education dimensions, along with the categories (or target groups) within each dimension."		X				
55. "A Framework to Integrate ICT Security Awareness into the South African Schooling System"	Walaza et al. (2014)	Qualitative	Conference paper	"This study deals with the problem of the lack of ICT security awareness in South African education (among South African learners)."				X		X
56. "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?"	Bada et al. (2015)	Qualitative		"The present paper focuses on Cyber Security Awareness Campaigns, and aims to identify key factors regarding security which may lead them to failing to appropriately change people's behaviour."		X				
57. "Development of a framework to leverage knowledge management systems to improve security awareness"	Lupiana (2008)	Qualitative	Masters dissertation	"This study investigated how to harness the power of users by developing a framework from which a knowledge management system was developed that provides a participatory education approach to security issues."	X			X		

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
58. "Enhancing Cyber Security for SME organizations through self-assessments: How self-assessment raises awareness"	Hassinen (2017)	Quantitative	Masters dissertation	"This thesis primarily studied the importance of self-assessment in increasing business organizations' cyber security awareness of their ICT environment."	X				X	
59. "A prototype for enhancing information security awareness in industry "	Kritzinger & Smith (2009)	Qualitative	Journal article	"This paper is principally aimed at expounding a prototype for the ISRA model to highlight the advantages of utilizing the model."		X				
60. "Design of a Cyber Security Awareness Campaign for internet Café Users in Rural Areas"	Labuschagne et al. (2011a)	Qualitative	Conference paper	"This paper addresses how the NIST framework, defined in the guide, "Building an Information Technology Security Awareness and Training Program", can be used to develop a security awareness program that focuses on possible cyber threats at internet Cafés."		X				X
61. "Cyber security for home users : a new way of protection through awareness enforcement"	Kritzinger & Von Solms (2010)	Qualitative	Journal paper	"This paper investigates the position of home users regarding information security awareness and proposes a new model the E-Awareness Model (E-AM)."			X			X
62. "Examining the effects of knowledge, attitude	Kaur & Mustafa (2013)	Quantitative	Conference paper	"This paper reports awareness of information security at a SME in Malaysia. The research aims	X				X	

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
and behaviour on information security awareness: A case on SME”				to establish the relationship between knowledge, attitude and behaviour and information security awareness.”						
63. “Individual differences and Information Security Awareness”	McCormac et al. (2017)	Quantitative	Journal article	“The main purpose of this study was to examine the relationship between individuals' Information Security Awareness (ISA) and individual difference variables, namely age, gender, personality and risk taking propensity.”	X					
64. “Investigating information system security policy and awareness training programs in South African organizations”	Makhudu et al. (2012)	Quantitative		“This paper discusses what organizations should do to make employees aware of their security policies and that organisations may face.”	X				X	
65. “Exploring the use of an e-learning environment to enhance information security awareness in a small company”	Holdsworth & Apeh (2017)	Qualitative	Conference paper	“This paper presents a structured approach for eliciting industry requirement for developing and implementing an immersive Cyber Security Awareness learning platform.”		X			X	
66. “A survey on cybersecurity	Tirumala et al. (2019)	Quantitative	Conference paper	Propose a framework that helps with the process of implementing cybersecurity awareness	X			X		



Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
awareness concerns, practices and conceptual measures”										
67. “Cyber safety awareness and culture planning in South Africa”	Kritzinger et al. (2018)	Qualitative	Conference paper	“To explore possible new trends in creating awareness among cyber users.”		X				X
68. “Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa”	Lejaka et al. (2019)	Qualitative	Conference paper	“To review, discover and update researchers about prior cyber security awareness (CSA) studies conducted in the context of South African SMMEs.”		X			X	X
69. “Cyber Security Awareness Among College Students”	Moallem (2019)	Quantitative	Conference paper	“To investigate student awareness and attitudes toward cyber security and the resulting risks in the most advanced technology environment.”	X					
70. “Cyber security awareness and culture in rural Norway”	Gunleifsen et al. (2019)	Quantitative	Conference paper	“To understand the level of security awareness, the perception, and the culture of users in aspects related to security.”	X					
71. “Cyber Security Situational Awareness among Parents”	Ahmad (2019)	Quantitative	Conference paper	“To measure the level of cyber security parental awareness to protect their children.”	X					

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
72. "Cyber Clinics: Re-imagining Cyber Security Awareness"	Croasdell et al. (2018)	Quantitative	Conference paper	"To examines cyber security awareness training with different awareness methods based on measurements of time, cost, personalization, relevance and interactivity."	X					
73. "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues"	Aldawood & Skinner (2019b)	Qualitative	Journal article	"To highlights pitfalls and ongoing issues that organizations encounter in the process of developing the human knowledge to protect from social engineering attacks."	X					
74. "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)"	Bada & Nurse (2019)	Qualitative	Journal article	"Proposes a high-level programme for cybersecurity education and awareness to be used when targeting Small-to-Medium-sized Enterprises/Businesses (SMEs/SMBs) at a city-level."			X		X	X
75. "Discussion on Cyber Security Awareness and Awareness Model Building Based on Connectionism"	Li et al. (2018)	Qualitative	Conference paper	"To discuss the meaning and formation of cyber security awareness and build awareness model based on connectionism."			X			

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
76. "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review"	Aldawood & Skinner (2019a)	Qualitative	Conference paper	"To identify various social engineering cyber security threats in diverse environments."		X				
77. "Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE"	Al Shamsi (2019)	Qualitative	Journal article	"To investigate the effectiveness of cyber security awareness program."		X				
78. "Framework of Raising Cyber Security Awareness"	Wang et al. (2019)	Quantitative	Conference paper	"To elaborates the connotation and research contents of cyber security awareness, proposes a cyber security awareness raising framework."				X		
79. "Mobile Information Security Awareness Among Students in Higher Education : An Exploratory Study"	Moletsane & Tsibolane (2020)	Quantitative	Conference paper	"This study assesses factors that impact mobile security awareness of students (N=397) at a higher education institution in South Africa."			X			X
80. "A Framework to Enhance ICT Security Through Education, Training & Awareness (ETA) Programmes in	Walaza et al. (2020)		Conference paper	"This research aims to explore the literature review that has been conducted; in an effort to propose a framework that will use of Education, Training & Awareness (ETA) programmes to		X			X	

Publication title	Authors	Methodology	Publication type	Research purpose	Measure	Design and evaluate	Models	Frameworks	SMMEs	Included in study
South African Small, Medium and Micro-sized Enterprises (SMMEs): A Scoping Review”				improve ICT security in South African small enterprises.”						

## 8.2 APPENDIX B: NO HUMANS INVOLVED (ETHICAL APPROVAL)



### UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) RESEARCH AND ETHICS COMMITTEE

29 August 2018

Ref #: 045/TKL/2018/CSET\_SOC  
Name: Mr Tebogo Kesetse Lejaka  
Student #: 46926461

Dear Mr Tebogo Kesetse Lejaka

**Decision: Ethics Approval for 3 years  
(No Humans involved)**

**Researchers:** Mr Tebogo Kesetse Lejaka,  
[46926461@mylife.unisa.ac.za](mailto:46926461@mylife.unisa.ac.za),

**Project Leader(s):** Dr Adele da Veiga, [dveiga@unisa.ac.za](mailto:dveiga@unisa.ac.za), +27 11 670 9175  
Prof Marianne Loock, [loockm@unisa.ac.za](mailto:loockm@unisa.ac.za), +27 11 670 9120

#### **Working Title of Research:**

A Conceptual Framework of Cyber Security Awareness for Small, Medium, and Micro Enterprises (SMMEs)

**Qualification:** MSc in Computing

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above mentioned research. Ethics approval is granted for a period of three years, from 29 August 2018 to 29 August 2021.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially



---

if those changes affect any of the study-related risks for the research participants. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.

3. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
4. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
5. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
6. No field work activities may continue after the expiry date (29 August 2021). Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

*Note:*

*The reference number 045/TKL/2018/CSET\_SOC should be clearly indicated on all forms of communication with the intended research participants, as well as with the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee.*

Yours sincerely

---

Dr. B Chimbo

Chair: Ethics Sub-Committee SoC, College of Science, Engineering and Technology (CSET)

---

Prof I. Osunmakinde

Director: School of Computing, CSET

---

Prof B. Mamba

Executive Dean: CSET

## 8.3 APPENDIX C: HUMANS INVOLVED (ETHICAL APPROVAL)



### UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

18 November 2020

ERC Reference #: 2020/CSET/SOC/030

Name: Tebogo Kesetse Lejaka

Student #: 46926461

Dear Mr TK Lejaka

**Decision: Ethics Approval from  
18 November 2020 to 17 November 2023  
(Humans involved)**

**Researcher** Mr Tebogo Kesetse Lejaka  
46926461@mylife.unisa.ac.za,

**Supervisors:** Prof. Adele da Veiga  
dveiga@unisa.ac.za, 011 670 9175  
Prof. Marianne Looock  
loockm@unisa.ac.za, 011 670 9120

**Working title of research:**

**Conceptual Framework for Cyber Security Awareness in Small, Medium, And Micro Enterprises**

**Qualification:** MSc in Computing

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **low risk application** was expedited by the College of Science, Engineering and Technology's (CSET) Ethics Review Committee on 18 November 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa COVID-19 position statement on research ethics attached.



University of South Africa  
Preller Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology's (CSET) Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date 17 November 2023. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.
9. Permission to conduct this research should be obtained from the CSIR and SAASTA prior to commencing field work.

**Note**

*The reference number 2020/CSET/SOC/030 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.*

Yours sincerely,

---

Dr C Pilkington  
Chair of School of Computing Ethics Review Subcommittee  
College of Science, Engineering and Technology (CSET)  
E-mail: [pilkid@unisa.ac.za](mailto:pilkid@unisa.ac.za) Tel: (011) 471-2130



University of South Africa  
Pretorius Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)



---

Prof. E Mnkandla  
Director: School of Computing  
College of Science Engineering and  
Technology (CSET)  
E-mail: [mnkane@unisa.ac.za](mailto:mnkane@unisa.ac.za)  
Tel: (011) 670 9104

---

Prof. B Mamba  
Executive Dean  
College of Science Engineering and  
Technology (CSET)  
E-mail: [mambabb@unisa.ac.za](mailto:mambabb@unisa.ac.za)  
Tel: (011) 670 9230



University of South Africa  
Pretter Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

## 8.4 APPENDIX D: PERMISSION LETTERS



### PERMISSION LETTER

**Request for permission to conduct research at The South Africa Agency for Science and Technology Advancement (SAASTA) | Science Awareness - Observatory**

A conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs)

12 August 2020

The South Africa Agency for Science and Technology Advancement (SAASTA)

Dear

My name is Tebogo Kesetse Lejaka and I am conducting research, under supervision of Prof Adéle da Veiga and Prof Marianne Looek towards a conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs), in the School of Computing, College of Science, Engineering and Technology at the University of South Africa (UNISA). The research study is funded from the Council for Scientific and Industrial Research (CSIR) and Department of Science and Innovation (DSI) for academic and other related fees. I hereby invite the SAASTA to participate in my study entitled "A conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs)". The involvement will relate to interviews with two to four staff members of the SAASTA within Science Awareness unit. If necessary, I would appreciate if you could assist with the identification and establishment of a connection with experts (in terms of their names, contact details and designations).

The aim of the study is to develop a conceptual framework for enhancing cyber security awareness in the community of South African SMMEs. This study is expected to collect information that could be used to validate the conceptual framework that can help in enhancing cyber security awareness knowledge within the community of South African SMMEs.



University of South Africa  
Pretter Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392, UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

PERMISSION LETTER

**Request for permission to conduct research at Council for Scientific and Industrial Research (CSIR)**

A conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs)

12 August 2020

Council for Scientific and Industrial Research (CSIR)

Dear

My name is Tebogo Kesetse Lejaka and I am conducting research, under supervision of Prof Adéle da Veiga and Prof Marianne Look towards a conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs), in the School of Computing, College of Science, Engineering and Technology at the University of South Africa (UNISA). The research study is funded from the Council for Scientific and Industrial Research (CSIR) and Department of Science and Innovation (DSI) for academic and other related fees. I hereby invite the CSIR to participate in my study entitled "A conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs)". The involvement will relate to interviews with two to four staff members of the CSIR. If necessary, I would appreciate if you could assist with the identification and establishment of a connection with experts (in terms of their names, contact details and designations).

The aim of the study is to develop a conceptual framework for enhancing cyber security awareness in the community of South African SMMEs. This study is expected to collect information that could be used to validate the conceptual framework that can help in enhancing cyber security awareness knowledge within the community of South African SMMEs.



## 8.5 APPENDIX E: CONSENT FORM



### CONSENT TO PARTICIPATE IN THIS STUDY

I, \_\_\_\_\_ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the interview process for validating the intermediate cs&4smmes (RSA) framework.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname \_\_\_\_\_

Participant signature \_\_\_\_\_ Date \_\_\_\_\_

Researcher's Name & Surname TEBOGO LEJAKA

Researcher's signature \_\_\_\_\_ Date 12 August 2020



## 8.6 APPENDIX F: PARTICIPANT INFORMATION SHEET



### PARTICIPANT INFORMATION SHEET

Ethics clearance reference number:

12 August 2020

Title: CONCEPTUAL FRAMEWORK FOR CYBER SECURITY AWARENESS IN SMALL, MEDIUM, AND MICRO ENTERPRISES (SMMEs)

#### Dear Prospective Participant

My name is Tebogo Kesetse Lejaka and I am conducting research, under supervision of Dr Adèle da Veiga and Prof Marianne Looock towards a conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs), in the School of Computing, College of Science, Engineering and Technology at the University of South Africa (UNISA). The research study is funding from the Council for Scientific and Industrial Research (CSIR) and Department of Science and Innovation (DSI) for academic and other related fees. I hereby inviting you to participate in a study entitled "A conceptual framework for cyber security awareness in Small, Medium, and Micro Enterprises (SMMEs)".

This study is expected to collect important information that could be used to validate a conceptual framework that can help in enhancing cyber security awareness knowledge within the community of South African SMMEs.

I have purposively selected knowledgeable professionals with experience in the research domain area and field of operation related to cyber security (both awareness and practice), science and technology awareness, and SMMEs management. I hereby confirm that you became one of the selected experts and your participation during the interview session would be greatly appreciated.

I will mainly identify experts within organisations such as the CSIR, NFR | SAASTA (permission will be acquired from respective organisations), and within South African SMMEs. In addition, I will mainly search and identify experts in SMMEs that are within my network or surrounding. Google search, Google Scholar, LinkedIn and other relevant social media platforms will be



University of South Africa  
Pretter Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

utilised if necessary. The experts will be identified, obtain their contact details, and send a formal invitation and other related documents in order for them to voluntarily participate into the study. If applicable, recommendation from other experts will be considered as well. Please note, the contact details were mainly requested for research purpose only.

In this study, a total of six to twelve expert reviewers (two to four experts from the CSIR, two to four experts from the NRF | SAASTA, two to four experts from SMMEs) are selected to attend an interview in order to validate the intermediate Csa4SmmeS {RSA} framework. The interview session is expected to take approximately two hour maximum, however you are allowed to terminate the interview at any given time. In addition, please note you are free to respond to questions you are comfortable with. With your permission, the interview will be recorded (as an audio or video based format) for the purpose of data analysis. However, if you wish not to be recorded, notes can be taken instead. If you agreed to be recorded, then you feel uncomfortable during the interview, the recording can be terminated with your request.

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. However, you will not be able to withdraw from the study once data is analysed and used to validate the intermediate Csa4SmmeS {RSA} framework. Please note that no individual identities will be used in any reports or publications resulting from the study.

Your opinion given during the interview is valuable and will be used to validate and improve the intermediate Csa4SmmeS {RSA} framework, which can help in enhancing cyber security awareness within the community of South African SMMEs. Please note that you will not be in any risk or discomfort because of your participation. Please note that you will not be paid for participating in this research.

Your responses during the interview will be kept confidential and no identities will be used. You have the right to insist that your name will not be recorder anywhere and that no one, apart from the researcher and identified members of the research team, will know about your involvement in this research. Your answers will be given a code number or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

All collected data will be stored by the researcher for a minimum period of five years in a secure place (cupboard/filing cabinet) for future research or academic purposes; electronic information



University of South Africa  
Preller Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
[www.unisa.ac.za](http://www.unisa.ac.za)

will be stored on a password protected computer. Hard copies will be shredded and electronic copies will be permanently deleted from the hard drive of the computer through the use of a relevant software programme. As with all research, there is a chance that confidentiality could be compromised; however, we are taking precautions to minimize this risk.

This study has received written approval from the Research Ethics Review Committee of the School of Computing under the College of Science, Engineering and Technology, UNISA. A copy of the approval letter can be obtained from the researcher if you so wish.

If you would like to be informed of the final research findings, please contact myself (Tebogo Kesetse Lejaka) on \_\_\_\_\_ or my email address 46926461@mylife.unisa.ac.za. The collected data will be permanently destroyed, however, the findings will be published in form of a dissertation. Therefore, the findings of the study will always be available. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Tebogo Kesetse Lejaka on \_\_\_\_\_ or email address 46926461@mylife.unisa.ac.za. Should you have concerns about the way in which the research has been conducted, you may contact Prof Adèle da Veiga on +27 11 647 9175 or email address dveiga@unisa.ac.za. Contact the research ethics chairperson of the School of Computing Research Ethics Committee: Mr. Colin Pilkington on 011 471 2130 or email address Pilkiol@unisa.ac.za if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.

Researcher's Name & Surname \_\_\_\_\_ Tebogo Lejaka \_\_\_\_\_

Researcher's signature \_\_\_\_\_ Date \_\_\_\_\_ 12 August 2020 \_\_\_\_\_



University of South Africa  
Peter Street, Muckleneuk Ridge, City of Tloane  
PO Box 392 UNISA 0003 South Africa  
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150  
www.unisa.ac.za

## 8.7 APPENDIX G: LANGUAGE EDITING CERTIFICATE

---

### DECLARATION BY LANGUAGE PRACTITIONER

I, Yvonne Smuts, hereby declare that I have been appointed by Tebogo Lejaka ("the candidate") to attend to the linguistic aspects of his dissertation that is hereby submitted in fulfilment of the requirements for the degree Master of Science in Computing at the University of South Africa.

To the best of my knowledge, all suggestions and recommendations made by me in this regard have been attended to by the candidate.

**Title of dissertation:** *A framework for cyber security awareness in small, medium and micro enterprises (SMMEs) in South Africa*

Date: 25 July 2021

(Ms) Y Smuts

*BA (Languages) (UP)*

*HED (cum laude) (UP)*

*SATI Accredited Member (No. 1002242)*

*Member of Prolingua*