Faculty of Computing and Informatics

Department of Informatics

Designing a National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation in Namibia

Thesis submitted in fulfilment of the requirements for the degree of

Master of Computer Science

at the

Namibia University of Science and Technology

Presented by:	**Diana J. Tjirare**
Student Number:	**200408585**
Supervisor:	**Dr. Fungai Bhunu Shava**
Co-Supervisor:	**None**
Submission Date:	**June 2018**

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Designing a National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation in Namibia

Presented by: Diana J. Tjirare

Thesis presented in fulfillment of the requirements for the degree of

Master of Computer Science

at the Namibia University of Science and Technology.

Supervisor: Dr. Fungai Bhunu Shava

Submission Date: June 2018

DECLARATION

I, Diana J. Tjirare born on the 01 May 1984 in Windhoek, Namibia hereby declare that the work contained in the report for my Master's project, entitled Designing a National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation in Namibia, is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree.

Signature: _____ Date: _____

SIGNATURE OF THE SUPERVISOR

I, _____, herewith declare that I supervised this research project.

Signature: _____ Date: _____

RETENTION AND USE OF THESIS

I, Diana J. Tjirare being a candidate for the degree of Master Computer Science accept the requirements of the Namibia University of Science and Technology relating to the retention and use of theses deposited in the Library and Information Services. In terms of these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purposes of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of theses/mini-theses.

Signature: _____ Date: _____

METADATA

TITLE:	Mrs.
STUDENT NAME:	Diana Jogbeth Tjirare
SUPERVISOR:	Dr Fungai Bhunu Shava
INSTITUTION:	Namibia University of Science and Technology
SCHOOL:	Faculty of Computing and Informatics
DEGREE:	Master of Computer Science: Information Security
KEYWORDS:	Information security, Information Security Management System, Information Security Policies, Policy framework, ISO/IEC 27000 series, Security policy
SUBJECT:	Designing a National Adoption Policy Framework for ISO/IEC 27000 standards implementation in Namibia
METHODOLOGY:	Design Science Research, Case Study, Survey, Questionnaire, Interview, Literature review
DOCUMENT DATE:	June 2018

ACKNOWLEDGEMENTS

Praise be to the Lord, for he has heard my cry for mercy. The Lord is my strength and my shield, my heart trust in him and he helps me. My heart leaps for joy, and with my song I praise him.

My sincere gratitude goes to my two pillars throughout this journey my supervisor Dr Fungai Bhunu Shava and my husband Mr. Wilson Tjirare. The thought of giving up often came up but you both pushed me to the finish line. Dr Fungai Bhunu Shava meeting you in January 2014 has been one of the greatest blessings. Thank you for your guidance, supervision, motivation, patience, encouragement, love, dedication towards me, believing in me, your support from the beginning until the end of this journey. Mr. Wilson Tjirare I thank God for a friend and husband. Thank you for your patience, love, strength, compassion, encouragement and support throughout this journey. My children Angel and Kuveri Tjirare thank you for your patients support and love. To my parents Fanuel and Gertrudt Ngutjinazo for your love and support. To my sisters Venaune Ngutjinazo, Okeri Ngutjinazo and Ngurimuje Ngutjinazo thank you for your support, patience, love and for baby-sitting Kuveri. To the employees of the Office of the Prime Minister (OPM), Ministry of Information and Communication Technology (MICT), Communication Regulatory Authority of Namibia (CRAN), Telecom Namibia (TN), Namibia Institute of Standards (NIS) and Namibia University of Science and Technology Master's students thank you for assisting to complete the survey for the project. Finally, I would offer my gratitude to all those who supported me in any way for the completion of my research project.

ABSTRACT

To ensure that the information asset is protected and available to organisations, information security needs to be governed by security standards. The ISO/IEC 27000 family of standards is one such standard; it keeps information assets secure and provides an information security management best practices framework.

An exploratory pilot survey conducted in 2015 with the key stakeholders namely the Communications Regulatory Authority, Namibia Institute of Standards, Internet Service Providers and government departments revealed that these standards are not being implemented despite their importance. Based on the literature review and the pilot study, the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia was evaluated. The study focused on the implementation extent for ISO 27000, 27001, 27002, 27003 and 27004 as these are the critical standards to the security posture of any organisation. It was established that there is no adoption of the ISO 27000 standards using the gap analysis strategy. Design Science Research methodology was used for this study, which involved the creation of new knowledge through the design of new artefacts and analysis of the use and/or performance of such artefacts. A qualitative case study research approach with security critical organisations in Namibia was used to collect and analyse data for this study. Surveys and interviews were used to collect data from purposefully identified key stakeholders. The stakeholders offered rich information about the phenomenon under study. The survey results were used to evaluate the extent of implementation and the factors contributing to the poor implementation. It was found out that proper documentation, adequate budget, resistant to change etc. play a critical role in influencing the adoption of the standards. A theoretical framework for ISO 27000 was derived from the findings and literature. The theoretical framework was evaluated and all participants agreed with the theoretical framework components and the framework itself. The framework was refined and an ISO/IEC 27000 family of standard national adoption policy framework was designed.

The national adoption policy framework for ISO/IEC 27000 standards implementation specific to Namibia will secure critical assets, manage risks more effectively, improve and maintain customer confidence, demonstrate conformance to international best practices, avoid brand damage and change its information security posture as technology is evolving.

Keywords: Information security, Information Security Management System, Information Security Policies, Policy framework, ISO/IEC 27000 series, Security policy

Table of Contents

DECLARATION iii

RETENTION AND USE OF THESIS iii

METADATA iv

ACKNOWLEDGEMENTS v

ABSTRACT vi

Chapter I – Introduction 1

1.1 Overview 1

1.2 Statement of the Problem 2

1.3 Purpose 3

1.4 Research Objectives and Questions 3

1.4.1 Research Questions 3

1.4.2 Research Objectives 3

1.5 Significance of the Study 4

1.6 Summary of Methodology 4

1.7 Limitations 5

1.8 Definition of Terms 5

1.8.1 Information Security Framework 5

1.8.2 Security Policy 5

1.8.3 Policy Framework 5

1.8.4 ISO/IEC 27000 6

1.8.5 Information Security 6

1.8.6 Information Security Policies 6

1.9 Chapter Outline 6

Chapter 2 – Literature Review 7

2.1 Introduction 7

2.2 Background 7

2.2.1 Computer and Data Security 8

2.2.2 Network Security 9

2.2.3 Information Security Management 10

2.3 Organisation Design and Strategy 13
2.4 People 15
2.5 Technology 16
2.6 Process 17
2.6.1 ISO/IEC 27000 Family of Standards 21
2.7 ISMS Implementation 30
2.7.1 Conducting a Gap Analysis 35
2.7.2 Define the Information Security Policy 37
2.7.3 Information Security Risk 39
2.8 Theoretical Framework 40
2.9 Summary 41
Chapter 3 – Methodology 43
3.1 Introduction 43
3.2 Research Process 44
3.2.1 Research Approach 44
3.2.2 Research Strategies 46
3.2.3 Time Horizons 58
3.3 Research Design- Design Science Research Strategy Overview 58
3.3.1 Design Science Research Methodologies 58
3.3.2 Design Science Research Process models 62
3.3.3 Design Science Research Strategy Application to this Research 65
3.4 Research Quality 70
3.4.1 Credibility 70
3.4.2 Transferability 71
3.4.3 Dependability 71
3.4.4 Confirmability 72
3.4.5 Trustworthiness 72
3.5 Ethical Considerations 72
3.5.1 Ethical Consent 72
3.5.2 Anonymity and Confidentiality 73
3.6 Summary 73
Chapter 4 – Data Collection and Results 74

4.1 Introduction 74
4.2 Literature Review 74
4.3 Interview 75
4.4 Summary 79
Chapter 5 – Framework Design Process 80
5.1 Introduction 80
5.2 Problem Identification and Motivation 81
5.3 Define the Objectives for a Solution 81
5.4 Design and Development 82
5.4.1 Theoretical Framework 82
5.4.2 Framework Implementation Guidelines 86
5.5 Demonstration 89
5.6 Evaluation 94
5.6.1 Framework Evaluation Tool Design 94
5.6.2 Framework Evaluation Tool Pilot Study 95
5.6.3 Framework Evaluation 96
5.6.4 Framework Evaluation Results 97
5.6.5 Summary of Findings 131
5.7 Communication 132
5.7.1 Information Security Policy 134
5.8 Summary 136
Chapter 6 - Conclusions 137
6.1 Introduction 137
6.2 Overview of the Study 137
6.3 Research Contributions 139
6.4 Limitations 140
6.5 Lesson Learnt 140
6.6 Reflections 141
6.6.1 Scientific Reflection 141
6.6.2 Methodological Reflection 142
6.6.3 Substantive Reflection 142
6.7 Possible Future Research 143

6.8 Conclusion 143
REFERENCES..... 145
APPENDIX A: REQUEST FOR PERMISSION TO CONDUCT RESEARCH 162
APPENDIX B: Semi-structured Interview Questions 164
APPENDIX C: Conference Paper..... 166
APPENDIX D: Framework Evaluation Tool 183
APPENDIX E: Framework Evaluation Results 200
APPENDIX F: Language Editor..... 249

List of Tables

Table 2.1 ISMS Pillars by different authors 12
Table 2.2 ISMS and Governance Framework Standards comparison 18
Table 2.3 ISO/IEC 27000 family of standards application to the study 22
Table 2.4 ISO/IEC 27001 requirements for each PDCA cycle stage 25
Table 2.5 ISMS Implementation Steps 31
Table 2.6 ISMS Implementation Steps divided into PDCA cycle 33
Table 2.7 Information Security Policy Structure 37
Table 3.1 Research Strategies 46
Table 3.2 Research questions and methods for the implementation of ISO/IEC 27000 48
Table 3.3 Sampling methods 51
Table 3.4 Data collection methods 53
Table 3.5 Data analysis methods 56
Table 3.6 Process models comparison 65
Table 3.7 Framework evaluation methods 68
Table 4.1 Collected data from semi-structured interviews 76
Table 4.2 Summary of semi-structured interview response and, the benefit and mitigating strategy of ISO/IEC 27000 78
Table 5.1 Use case scenarios for PLAN 91
Table 5.2 Stakeholders' Gender 97
Table 5.3 Stakeholders' age group 98
Table 5.4 Stakeholders' Position 98
Table 5.5 Stakeholders' years of experiences in information technology 99
Table 5.6 Stakeholders Organisation 99
Table 5.7 Total matching response and percentage importance 103
Table 5.8 Results of different security controls 108

Table 5.9 Security landscape of Namibia findings - Importance 114
Table 5.10 What is needed - Total percentage of matching responses 116
Table 5.11 Mitigating strategy - Total percentage of matching responses 118
Table 5.12 Factors affecting the adoption of the standard - Total percentage of matching responses 121
Table 5.13 Benefits of implementing ISO/IEC 27000 family of standards - Total percentage of matching responses 124
Table 5.14 Security Controls - Total percentage of matching responses 127
Table 5.15 Overall Framework Evaluation - Total percentage responses 129
Table 6.1 Research questions, research objectives, sampling methods and data collection methods 138
Table 6.2 Research question, answers and evidence 144

List of Figures

Figure 2.1 Information Security Components 8
Figure 2.2 BMIS Components 10
Figure 2.3 ISMS Pillars 11
Figure 2.4 Attacked users 14
Figure 2.5 World distribution of ISO/IEC 27001 certificates in 2014 16
Figure 2.6 ISO/IEC 27000 family of standard timeline 21
Figure 3.1 Inductive approach research steps 44
Figure 3.2 Deductive approach research steps 45
Figure 3.3 Types of case study designs 50
Figure 3.4 Method framework for design science research 59
Figure 3.5 Design Science Research Cycles 60
Figure 3.6 DSR Canvas 61
Figure 3.7 Design Science Research cycles application to the study 62
Figure 3.8 DSR process model 63
Figure 3.9 DSR process model 64
Figure 3.10 Process Model Application 66
Figure 5.1 Theoretical Framework 85
Figure 5.2 National adoption policy framework implementation guidelines 87
Figure 5.3 Implementation of the ISO/IEC 27001 90
Figure 5.4 Pilot Survey Data 1 95
Figure 5.5 Pilot Survey Data 2 95
Figure 5.6 Pilot Survey Data 3 96
Figure 5.7 ISO/IEC 27001 control domains, control objectives and controls 112
Figure 5.8 Final Results: Security landscape of Namibia 115
Figure 5.9 Final Results: What is needed to mitigate information security risk 117

Figure 5.10 Final Results: Mitigating strategy 119
Figure 5.11 Factors affecting the adoption of the standard 122
Figure 5.12 Benefits of implementing ISO/IEC 27000 family of standards 125
Figure 5.13 Security Controls 128
Figure 5.14 Overall Framework Evaluation 130
Figure 5.15 National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation 133

Abbreviations

CIRT	Computer Incident Response Team
COBIT	Control Objectives for Information and Related Technology
CRAN	Communication Regulatory Authority of Namibia
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Providers
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MICT	Ministry of Information and Communication Technology
NamCIRT	Namibia National Computer Incident Response Team
NIS	Namibia Institute of Standards
NIST	National Institute of Standards and Technology
NSI	Namibian Standard Institution
OPM	Office of the Prime Minister
PDCA	Plan Do Check Act
TN	Telecom Namibia

Chapter I – Introduction

1.1 Overview

The internet is considered the best way for communication by most organisations but it is not necessarily the best as there are many threats such as data modification, hacking and sniffing on local networks, virus infection, confidential data disclosure etc. which encountered while connected to the internet (Spruit & Samwel, n.d.). According to Internet World Stats (2011), internet usage in Namibia grew by 100% from the year 2000 to the year 2017 (Lourens, 2018). To mitigate the cyber security threats in Namibian organisations, information must be managed well. International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27000 family of standards is used for information security management together with other standards. "The ISO 27000 family of standards helps organizations keep information assets secure" (ISO, n.d.). eFortresses (n.d.) (as cited by Tjirare & Bhunu Shava, 2017) states that the ISO 27000 family of standards provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System.

One of the most important factors an organisation should devote its time and resource is data protection. ISO/IEC 27000 family of standards is used to manage information. Information that is not properly managed can be a threat to an organisation and currently there is poor or no adoption of ISO/IEC 27000 standards in the Namibian industry.

Namibian Standards Institution (NSI) is a national organisation accountable for regulating standards and quality assurance in Namibia to enhance industrial efficiency and productivity and it's a member of the ISO organisation (ISO, n.d.). In order to benefit from the ISO 27000 family of standards, the Namibian industry should adopt the ISO/IEC 27000 policy framework to mitigate the risks.

This section focused on the overview of the importance of the ISO/IEC 27000 family of standards in Namibian organisation to manage information and mitigate information risk The study focusses on ISO/IEC 27000, 27001, 27002, 27003 and 27004 as these are the critical standards to adopt first. The next sections will focus on the ISO/IEC 27000 family problem in Namibia, the purpose of the study, research questions and objectives, significance of the study, summary of the methodology used to solve the problem, study limitations, definitions of terms used for this study and finally the chapters' outline.

1.2 Statement of the Problem

Namibian organisations lack the usage and adoption of the ISO/IEC 27000 standards. This is supported by a preliminary survey with selected stakeholders namely the Communication Regulatory Authority of Namibia (CRAN), Telecom Namibia, Office of the Prime Minister (OPM), Ministry of Information and Communication Technology (MICT) and NSI, who revealed that these standards are missing. According to Uudhila (2016), the lack of cyber security best practices in the Namibian government institutes has made it difficult for IT staff to govern the security of different Information Systems and networks.

Namibia was the second most attacked country in November 2015 and this was revealed by Check Point Software Technologies, which found that Namibia was the country most targeted by cybercriminals during December of 2015 (IT News Africa, 2016). Granneman (2013) describes an information security framework as documented policies and procedures on the implementation and continuous improvement of the information security controls. The implementation of framework assists to mitigate the information security risk and reduce vulnerabilities in organisations (Granneman, 2013). The ISO/IEC 27000 family of standards provides a globally recognised information security management framework best-practice (ItGovernance, 2015).

Since Namibia is rated as one of the most vulnerable countries to cyber criminals, it certainly needs to implement these best practices to ensure secure cyber experiences. Namibia, as one of the most vulnerable countries to cyber criminals therefore needs to implement these best practises to guarantee safe cyber experiences for everyone.

1.3 Purpose

The purpose of this study is to understand the factors affecting the adoption of the ISO/IEC 27000 family of standards and propose a policy framework that will guide the adoption of the ISO/IEC 27000 family of standards in Namibia. The framework has to ensure that information security best practices are used in Namibian organisations to mitigate information security risks (Tjirare & Bhunu Shava, 2017). The study focusses on ISO/IEC 27000, 27001, 27002, 27003 and 27004 as these are the critical standards to adopt first.

1.4 Research Objectives and Questions

The next sub-sections will list the research questions and objectives used to guide the study.

1.4.1 Research Questions

- ✓ What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?
- ✓ What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?
- ✓ How can a policy framework be constituted to guide the adoption of ISO/IEC 27000 family of standards into security practice?

1.4.2 Research Objectives

- ✓ Investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia
- ✓ Investigate the factors affecting the adoption of ISO/IEC 27000 family of standards
- ✓ Design a policy framework to guide the adoption of ISO/IEC 27000 security standards in the practice

1.5 Significance of the Study

The study designed a national adoption policy framework for ISO/IEC 27000 standards implementation specific to Namibia, based on the ISO 27000, 27001, 27002, 27003 and 27004 that can assist organisations to gain the ISO 27000 family of standards benefits.

The ISO 27000 family of standards provides the following benefits to organisations and the Namibian organisations will gain similar benefits if they adopt and implement the ISO/IEC 27000 family of standards (ItGovernance, 2015) as follows:

- ✓ Critical assets are secured
- ✓ Risks are managed more efficiently
- ✓ Customer confidence is improved and maintained
- ✓ Provides compliance to universal best practices
- ✓ Avoidance of brand damage, loss of earnings or potential regulatory fines
- ✓ As technology develops, the organisation will change its information security posture

1.6 Summary of Methodology

Design Science Research methodology was used for this study, which deals with the creation of new knowledge through the design of new artefacts and an analysis of the use and/or performance of such artefacts. A qualitative case study research using an inductive approach with security critical organisations in Namibia was used to collect and analyse data for this study.

Interviews with selected stakeholders and literature reviews were used to evaluate the extent of implementation, the factors contributing to the poor implementation and informing the design of the framework. The framework was evaluated with an evaluation tool using surveys to find out the relevance of the framework. The stakeholders offered rich information about the phenomenon under study and confirmed that the framework was relevant.

1.7 Limitations

A cross sectional study involves the collection of data for a specific time period while a longitudinal study data is collected repeatedly over a period of time (Rouse, 2013; UK Essays, 2015). A cross sectional study was conducted which was limited to a case analysis of identified stakeholders to implement an ISO/IEC 27000 policy framework for security standards in Namibia. A longitudinal study should thus be conducted within Namibian organisations to allow for the generalisability of the framework. Several literatures were studied on the standards used elsewhere but the policy framework implemented is specific to Namibia.

1.8 Definition of Terms

1.8.1 Information Security Framework

An information security framework is a series of documented policies and procedures about the implementation and continuous improvement of information security controls in an organisational environment (Granneman, 2013).

1.8.2 Security Policy

A security policy is a document that outlines how an organisation will govern, protect and allocate its confidential information for computer network access (Webopedia, 2015).

1.8.3 Policy Framework

A set of standards and on-going goals that frame the premise of making rules and guidelines, and to give general direction to planning and improvement of the organisation (BusinessDictionary, 2015).

1.8.4 ISO/IEC 27000

ISO/IEC 27000 provides an overview of information security management systems (ISMS), which makes the topic of the ISMS family of standards and defines related terms (ISO, 2014).

1.8.5 Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel, 2013).

1.8.6 Information Security Policies

A collection of directives, regulations, rules, and practices that recommend how an organisation governs, protects, and distributes information (Kissel, 2013).

1.9 Chapter Outline

The study is divided into six chapters. Chapter one discusses the study overview, the research problem, purpose of the study, research objectives and questions, significance of the study, methodology summary, research limitations and definition of terms. Chapter two discusses different literatures relevant to the study. Chapter three focusses on the different methodologies used to answer the research questions and achieve the research objectives. The chapter focusses on the research approach, research strategy, research choice, time horizons, data collection and analysis methods, design science research strategy and the study's ethical considerations. Chapter four discusses the data collected using literature reviews and interviews with selected stakeholders and its analyses. Chapter five discusses the framework design process and the framework implementation guidelines. The last chapter, chapter six includes the study's conclusion and recommendations for future research.

Chapter 2 – Literature Review

2.1 Introduction

Chapter one specified the research project overview, purpose, research questions and objectives, significance of the study and the study limitations. This chapter discusses literature relevant to the study. The chapter briefly mentions different standards used in information technology governance and discusses the ISO/IEC 27000 family of standards in detail as the study focused on designing a national adoption policy framework for ISO/IEC 27000 standards implementation. Focus will be placed on discussing the supporting elements of the Information Security Management Systems (ISMS) referred to as pillars (Dutton, 2017). The related work is presented as follows: section 2.2 presents the information security background, section 2.3 presents the organisation design and strategy pillar, section 2.4 presents the people's pillar, section 2.5 presents the technology pillar, section 2.6 presents the process pillar, section 2.7 presents the Information Security Management System (ISMS) implementation, section 2.8 presents the theoretical framework and section 2.9 presents the chapter summary.

2.2 Background

The study focused on the information security domain. Whitman and Mattord (2012) define security as the protection against enemies who would do harm intentionally or unintentionally. For an organisation to be successful it should implement multiple layers of security namely (Whitman & Mattord, 2012):

- ✓ Physical security
- ✓ Personnel security
- ✓ Operations security
- ✓ Communications security
- ✓ Network security
- ✓ Information security

The information security layer is the focal point in this study. Whitman and Mattord (2012) state that information technology consists of the following components: information security management, computer and data security, and network security. Figure 2.1 depicts the information security components. At the heart of all these are policies which are used to ensure that organisational end users and IT infrastructure comply with information security requirements.

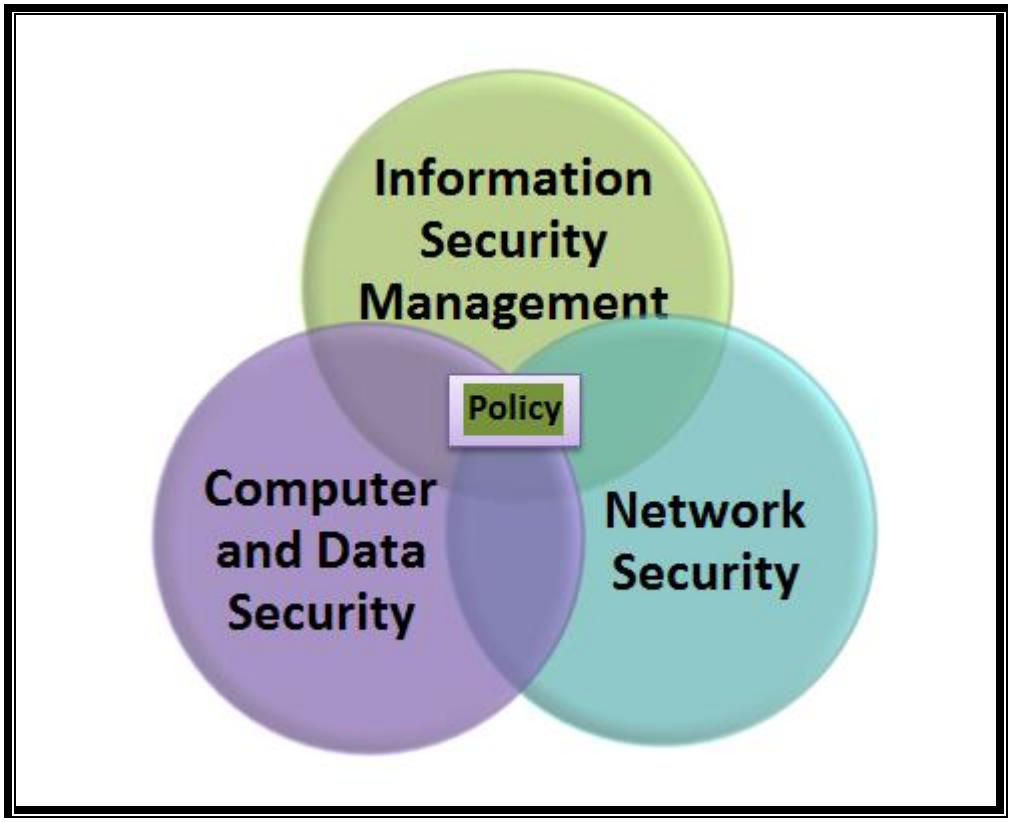


Figure 2.1 Information Security Components (Whitman & Mattord, 2012)

These components are discussed in the following subsections.

2.2.1 Computer and Data Security

Computer security is the protection of data, software, hardware, and firmware (components of computer systems), ensuring data integrity, limiting access to authorised users, and maintaining data confidentiality (Barnatt, 2017; Gunnels, 2018). They are controls that provide confidentiality, integrity, and availability to components of computer systems (Gunnels, 2018).

Data security is the protection of digital data from attacks, accidental deletion, security breaches and unauthorized access in storage, transit or in use (Diego, 2018).

Newitz (2015) suggests ways of computer and data security that can mitigate information security risks in organisations as follows:

- ✓ A strong password can prevent most attacks
- ✓ A new device can also be harmful
- ✓ The best software can also have security vulnerabilities
- ✓ Every website and app should use HTTPS
- ✓ The cloud is not safe — it just creates new security problems
- ✓ Software updates are crucial for your protection
- ✓ Hackers are not criminals
- ✓ Cyberattacks and cyberterrorism are exceedingly rare
- ✓ Darknet and Deepweb are not the same thing

2.2.2 Network Security

Network Security is the protection of networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure through physical and software preventative measures (SANS, 2018).

To protect network infrastructure, the following physical access controls from Lehtinen, Russell and Gangemi (2006) exist:

- ✓ Controlling physical access to the servers
- ✓ Controlling physical access to networked workstations
- ✓ Controlling physical access to network devices
- ✓ Controlling physical access to the cable
- ✓ Being aware of security considerations with wireless media
- ✓ Being aware of security considerations related to portable computers

- ✓ Recognizing the security risk of allowing data to be printed out
- ✓ Recognizing the security risks involving floppy disks, CDs, tapes, and other removable media

2.2.3 Information Security Management

Information security management (ISM) deals with making decisions to mitigate information security risks, making sure that security controls are implemented in organisations to mitigate information security risks and proposes security strategies (Vogel, 2014). ISM is linked to the implementation, project planning, policy enforcement and resource utilisation of an Information Security Management Systems (ISMS) (Vogel, 2014). An ISMS is a framework that states the policies and procedures used to manage tasks and activities to mitigate information security risks in an organisation and limiting security gaps (BSI, 2008; Techopedia, 2018a). ISMS use a holistic Business model for information security (BMIS) to manage its tasks and activities (ISACA, 2009). BMIS consist of the following components: organisation, people, process and technology as depicted in figure 2.2.

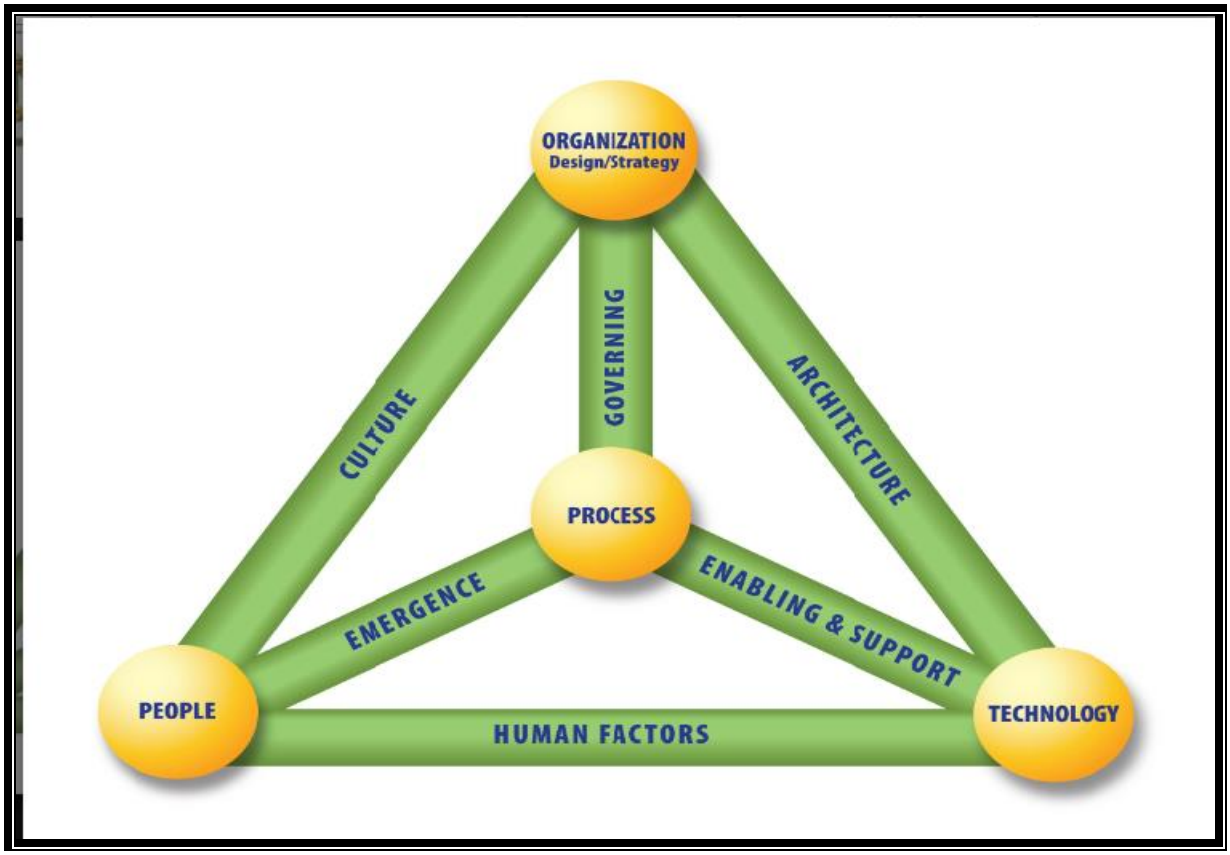


Figure 2.2 BMIS Components (ISACA, 2009)

According to Janes (2012), data loss in organisation is believed to be an Information Technology issue and the technology component should fix the problem. Janes (2012) further states that to mitigate data loss, organisations should not only focus on technology components but on people, processes and technology (Janes, 2012). Dutton (2017) refers to the people, processes and technology components as the ISMS pillars and they are used for an effective and robust information security. Ford (2013) says that an ISMS which addresses people, processes and technology is needed to properly secure an organisation. Figure 2.3 lists the requirements of the three pillars to mitigate information security risks.

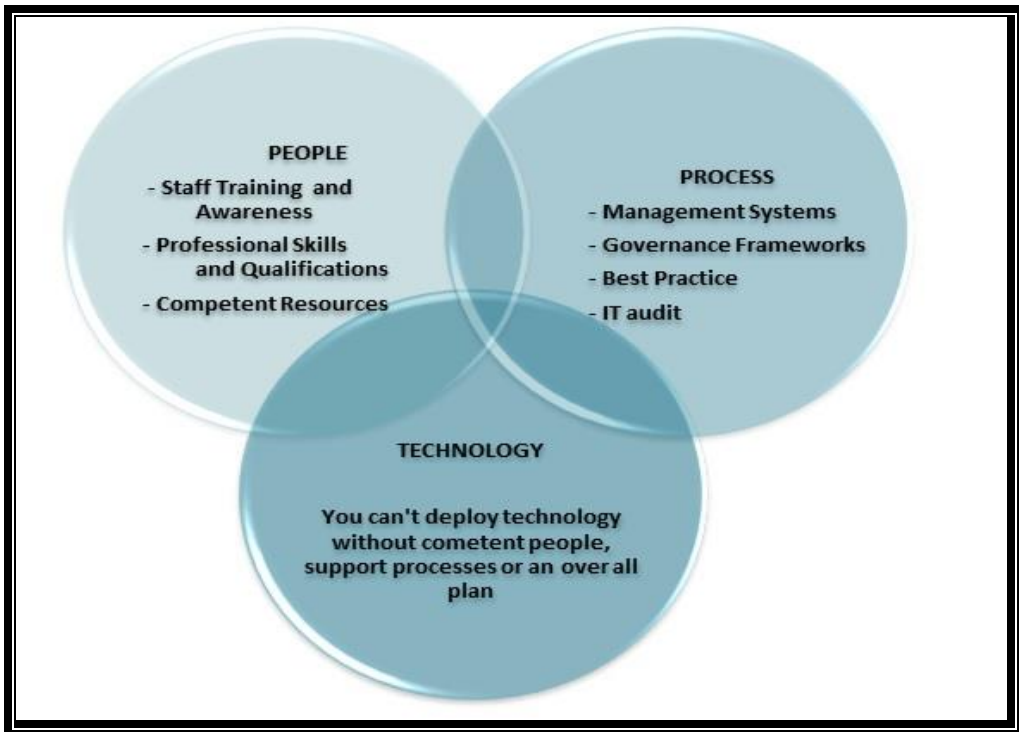


Figure 2.3 ISMS Pillars (Dutton, 2017)

The organisation, people, processes and technology components are referred to as ISMS pillars and their application for this study will be discussed in the next sections.

Table 2.1 presents views on the ISMS pillars from different authors and the relevance of their framework/model in addressing organisational security needs. The authors identify similar pillars which confirm that these are the important pillars for the security posture of Namibian organisation. This study considered the ISMS pillars as an important component when implementing the national adoption policy framework for ISO/IEC 27000 standards and it was added to the framework implementation guidelines. The importance of the ISMS pillars when implementing national adoption policy framework for ISO/IEC 27000 standards are discussed in section 5.4.2.2.

Table 2.1 ISMS Pillars by different authors

ISMS Pillars	Framework/Model	Authors	Relevance
People, Processes and Technology	Three pillars of cyber security	Dutton (2017)	Effective and robust cyber security requires an information security management system (ISMS) built on three pillars.
	Three pillars of a successful security strategy	Singh (2017)	State that ISMS, Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) fall under the processes pillar.
	People, process, and technologies impact on information data loss	Janes (2012)	To mitigate Information security risk the focus should be on all three ISMS pillars.
	People, processes and technology: the cyber security trinity	Ford (2013)	ISO27001 use an integrated approach and contain the ISMS pillars

2.3 Organisation Design and Strategy

The organisation design and strategy pillar consists of three parts namely the organisation, design and the strategy. An organisation is a group of people, assets and processes working together for the same goal (ISACA, 2009). Design defines how the strategy is implemented in an organisation (ISACA, 2009). Strategy specifies organisational objectives, goals, values and missions accomplished with different resources (ISACA, 2009).

Preliminary interviews with selected stakeholders in Namibia conducted in 2015 revealed that there is a lack/no implementation of the ISO/IEC 27000 family of standards in Namibian organisations.
Namibia is a country found on the south west part of Africa, formerly known as South West Africa, with a population of 2,6 million people as of April 2018 (Countrymeters, 2018; Green, 2018). Namibia upgraded the phase 2 of the West Africa Cable System (WACS) in September 2015, and the bandwidth was upgraded to 480Gbps, which means faster internet connection for Namibia and the whole SADC region (Kathindi, 2015). Namibia internet users grew by more than 100% from the year 2000 (Internet World Stats, 2015). Namibia is in the process of drafting a cyber-security bill and it was tabled in parliament in February 2017 (Smith, 2018). The bill was withdrawn from parliament for public input (Olivier, 2017). According to Federico in the paper written by Smith (2018), the cyber-security bill does not follow the international and local guidelines.

Namibia was ranked number seven for countries that have the most users attacked by banking Trojans with 9.3% of attacks as depicted in figure 2.4 (Kaspersky, 2015). Namibia was also ranked as the second country after Saudi Arabia in the ranking of countries with the most cyber-attacks (Bizcommunity, 2015).

Country	% Attacked users
Singapore	11.6
Austria	10.6
Switerzland	10.6
Australia	10.1
New Zealand	10.0
Brazil	9.8
Namibia	9.3
Hong Kong	9.0
South Africa	8.2
Lebanon	6.6

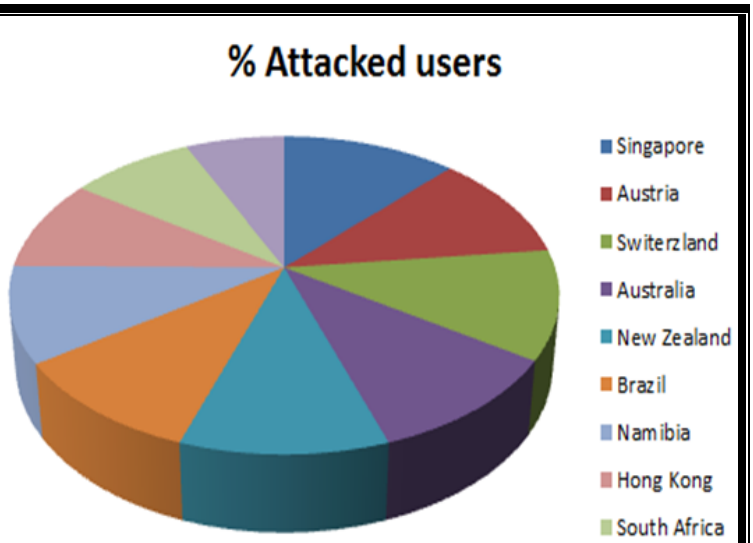


Figure 2.4 Attacked users (Kaspersky, 2015)

Namibia just started setting its information security best practise strategy by designing their cyber-security bill but it was withdrawn from parliament as discussed above. Namibia is already ranked as the second most cyber attacked country in the world and it is ranked number seven for countries that have the most users attacked by banking Trojan hence it must implement information security best practices. To protect data and have high quality data, information security management is needed. ISO/IEC 27000 family of standards is one of the ISM standards and the ISM standards are discussed in later sections. The purpose of the study was to design a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia that will mitigate information security risks in Namibian organisations. The national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia is therefore recommended for the cyber-security bill to follow international and local guidelines.

2.4 People

The people's pillar is about the human resources and their problems (ISACA, 2009). Dutton (2017) says that the people's pillar consists of two parts, first everyone in an organisation who needs an effective information security awareness program, who needs to know their role in preventing and reducing information security threats. And secondly the information security employees (specialists) who need the latest skills and qualifications to ensure that appropriate controls, technologies and practices are implemented to mitigate information security risks (Dutton, 2017). Employees that are not up to date with security qualifications and personal upgrading will not assist the organisation to mitigate information security risks by responding to cyber-attacks (Dutton, 2017).

To address these two elements, a Namibia National Computer Incident Response Team (NamCIRT) was proposed (ITU, 2017). The CIRT will be responsible for organizing cyber security events for responding to cyber-attacks in the country (Olivier, 2017). NamCIRT is responsible for (ITU, 2017):

- ✓ A single point of contact for reporting to incidents and incident coordination
- ✓ Helping the population and general computing community in preventing and handling computer security incidents
- ✓ Disseminating information and lessons learned to its users, other CIRT or response teams, as well as other appropriate organisations and international actors

NamCIRT alone will not be effective without standard compliance within the different organisations. Standards and frameworks for baseline security compliance have been designed by NIST for the USA, and ISO/IEC for the entire world. These standards and frameworks provide for human security aspects. According to Haseeb (2016), ISO conducted a survey in 2014 on how many people are certified on ISO/IEC 27001 and Namibia had no single certified person as depicted in figure 2.5. For the CIRT to successfully implement information security best practices the members should be trained and certified in information security qualifications and ISO/IEC 27001 certification is one such qualification.

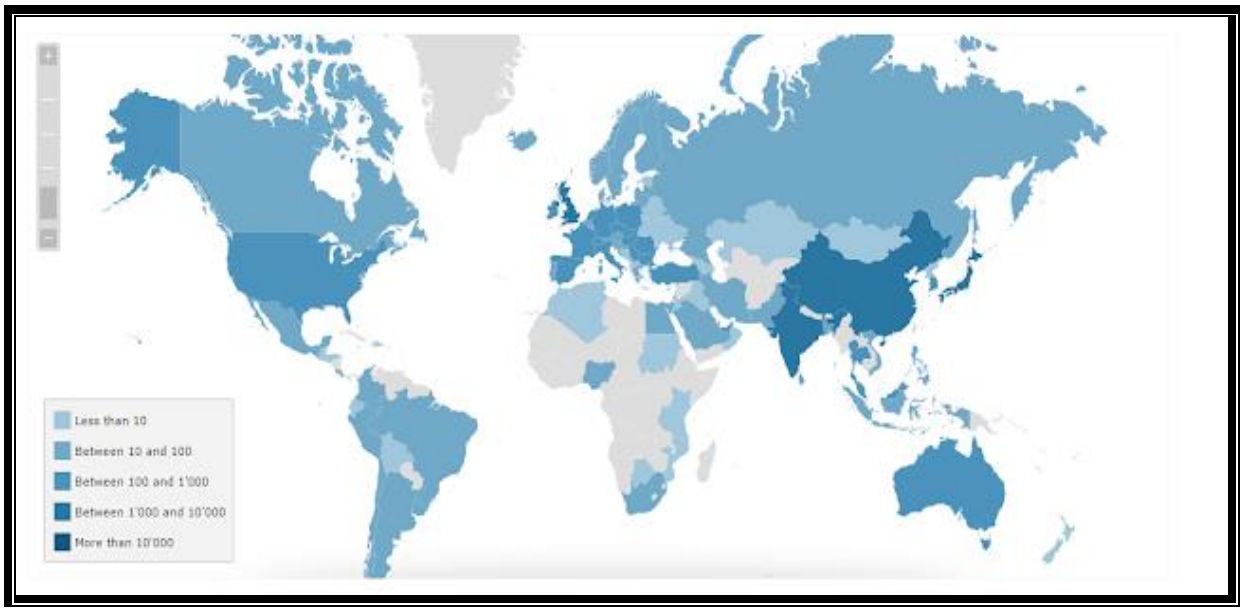


Figure 2.5 World distribution of ISO/IEC 27001 certificates in 2014 (Haseeb, 2016)

2.5 Technology

The technology pillar represents the tools, applications and infrastructure that make the processes more efficient (ISACA, 2009). Singh (2017) mentions a number of terms and technologies that can cause harm to an information security environment if not properly managed, namely: browser vulnerabilities, Bring Your Our Device (BYOD), lost or stolen devices, phishing attacks, data backups, desktop security and viruses, firewalls, VPNs and secure remote access, secure wireless connections, and network and server configurations. According to ITU (2017), cybersecurity incidents occurring in Namibia are currently not tracked or understood, and common types of cybersecurity incidents are related to:

- ✓ Scams
- ✓ Phishing
- ✓ Finance
- ✓ Viruses and worms
- ✓ Frauds (including in the Mobile networks)
- ✓ Web defacement

- ✓ Denial of Service

There is need for technology adoption and security policies to be designed for organisations to ensure CIA of information, and this is enabled by functional processes.

2.6 Process

The process pillar consists of the information security management systems (ISMS) and governance frameworks (Dutton, 2017). Processes are important pillars to the implementation of information security strategies that are continually reviewed and that define how organisations use the roles, activities and documentation to mitigate information security risks (Dutton, 2017).

An ISMS is a systematic approach that consists of policies and procedures used for managing sensitive organisational data to reduce information security risks and to ensure business endurance (Rouse, 2011). ISO/IEC 27001 is a requirement for creating ISMS which suggest documentation, internal audits, continual improvement and corrective and preventive action (Rouse, 2011). ISO/IEC 27001 belongs to the ISO/IEC 27000 family of standards and when used together, they specify the complete implementation of ISMS to all types and sizes of organisations (DCC, 2015; Granneman, 2013).

A governance framework is a formal framework that provides the alignment of Information Technology (IT) strategy with business strategy to produce measurable outcomes for obtaining organisational strategies and goals (Lindros, 2017). According to Lindros (2017), three IT governance frameworks exist namely:

COBIT (Control Objectives for Information and Related Technology) – A comprehensive framework with their roots in IT auditing and with the latest version COBIT 5 and they focus on risk management and mitigation.

ITIL (Information Technology Infrastructure Library) – Deals with IT service management to make sure that IT supports essential processes of the organisation.

NIST 800-53 (National Institute of Standards and Technology 800-53, Recommended Security Controls for Federal Information Systems) – Responsible for security controls for central information systems and organisations, and documents security controls for all federal information systems, except those designed for national security (Johnson et al., 2006; Techopedia, 2018b).

Table 2.2 compares the ISMS and governance framework standards. The following criteria are listed for each standard: organisation, function, main implementation area, implementation guidelines and whether information security risk assessment is conducted. The criteria explanation will follow after the table.

Table 2.2 ISMS and Governance Framework Standards comparison

Standard	COBIT	ITIL	NIST 800-53	ISO/IEC 27000 family of standards
Organisation	Information Systems Audit and Control Association (ISACA) (Gönderi, 2016)	Office of Government Commerce (OGC) (Gönderi, 2016)	United States Commerce Department (Lord, 2017)	International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) (Gönderi, 2016)
Function	Mapping IT Process (Gönderi, 2016)	Mapping IT Service Level Management (Gönderi, 2016)	Protects United States national information systems and organisations (Lord, 2017)	Information Security Framework (Gönderi, 2016)
Implementation	Information System Audit (Gönderi, 2016)	Manage Service level (Gönderi, 2016)	Enhance the information systems security used by national government	Compliance to security standard (Gönderi, 2016)

Standard	COBIT	ITIL	NIST 800-53	ISO/IEC 27000 family of standards
			(Lord, 2017)	
Implementation guidelines	Does not provide detailed guidelines to accomplish the control objectives (Gönderi, 2016)	Standards states what should be achieved (Gönderi, 2016)	Focuses on the plan and implementation phase only (Kosutic, 2014).	Provides detailed methods and practices of implementing an ISMS (Gönderi, 2016)
Information Security risk assessment	With COBIT 5 it focuses on information security risk assessment and mitigation by integrating ISO/IEC 27001 in their Information Security Model (Frisken, 2015).	ITIL service management identifies most of the security controls in ISO/IEC 27001. References ISO/IEC 27001 and the requirement of the ISMS (Warren, 2010)	Use multi-tiered approach to information security risk management (Lord, 2017)	Conducting an information security risk assessment is essential to ISO/IEC 27001 ISMS Biscoe (2017a)

Considering the current security landscape in Namibia as discussed under the organisation design and strategy pillar, the people's pillar and technology pillar, there is a need to consider policy frameworks that can guide the adoption of information security best practices to mitigate information security risks. Table 2.1 presented different criteria of ISMS and governance frameworks and standards. The criteria for each standard will be discussed below so as to select the standard that will be used to improve Namibia's security landscape:

Organisation: These are the different organisation that owns the standards.

Function: ISO/IEC 27000 family standards are used for Information Security framework while COBIT and ITIL are used for Mapping IT Process and Mapping IT Service Level Management. NIST 800-53 is used to protect the United States of America national information systems and organisations.

Implementation: ISO/IEC 27000 family standards is compliant to security standards. NIST 800-53 enhances the information systems security used by the United States of America national government

Implementation guidelines: COBIT stipulates what an Information Security Governance should achieve but it does not state how it should be achieved where as ITIL and the ISO/IEC 27000 family of standards states what should be achieved (Quizlet, n.d.).

ITIL provides best practices to align IT resources and assistance to business goals while ISO/IEC 27000 family of standards consists of a management system that controls information security and provides specific information security controls (The Agnosticator, 2013).

NIST 800-53 provides a better structure for security areas to be implemented and the exact security profiles to be achieved, whereas ISO/IEC 27000 family standards provide a broader picture for designing a system which protects all types of information, define which documents and records are needed, and use the Plan-Do-Check-Act (PDCA) cycle as the implementation methodology (Kosutic, 2014). The PDCA cycle is discussed under section 2.4.2.1.

Information Security risk assessment: COBIT and ITIL integrate/reference ISO/IEC 27001 for their information security risk management. NIST 800-53 use a multi-tiered approach to information security risk management. ISO/IEC 27000 family of standards use one of the standards for information security risk management.

The comparison above stipulates ISO/IEC 27000 family of standards and NIST 800-53 to be the only two standards that are used for information security. ISO/IEC 27000 family standards was selected for this study over NIST 800-53 as it provides detailed methods and practices for implementing the standard. ISO/IEC 27000 family standards provide a broader picture for designing a system and focus on the PDCA cycle whereas the NIST 800-53 focus on the plan and implementation phase only. The research project aimed to design a policy framework that can guide the adoption of information security best practices to mitigate information security risks.

The next section will discuss the ISO/IEC 27000 family of standards.

2.6.1 ISO/IEC 27000 Family of Standards

ISO 27000 family of standards was originally published as British Standard 7799 in 1995 and then later as ISO 17799 (Vanderburg, n.d.). DCC (2015) states that the policies, procedures, human and machine resources which constitute ISMS should ensure that the CIA Triad (Confidentiality, Integrity and Availability) is maintained across an organisation's physical, personal and organisational layers. Figure 2.6 presents the ISO/IEC 27000 family of standards timelines.

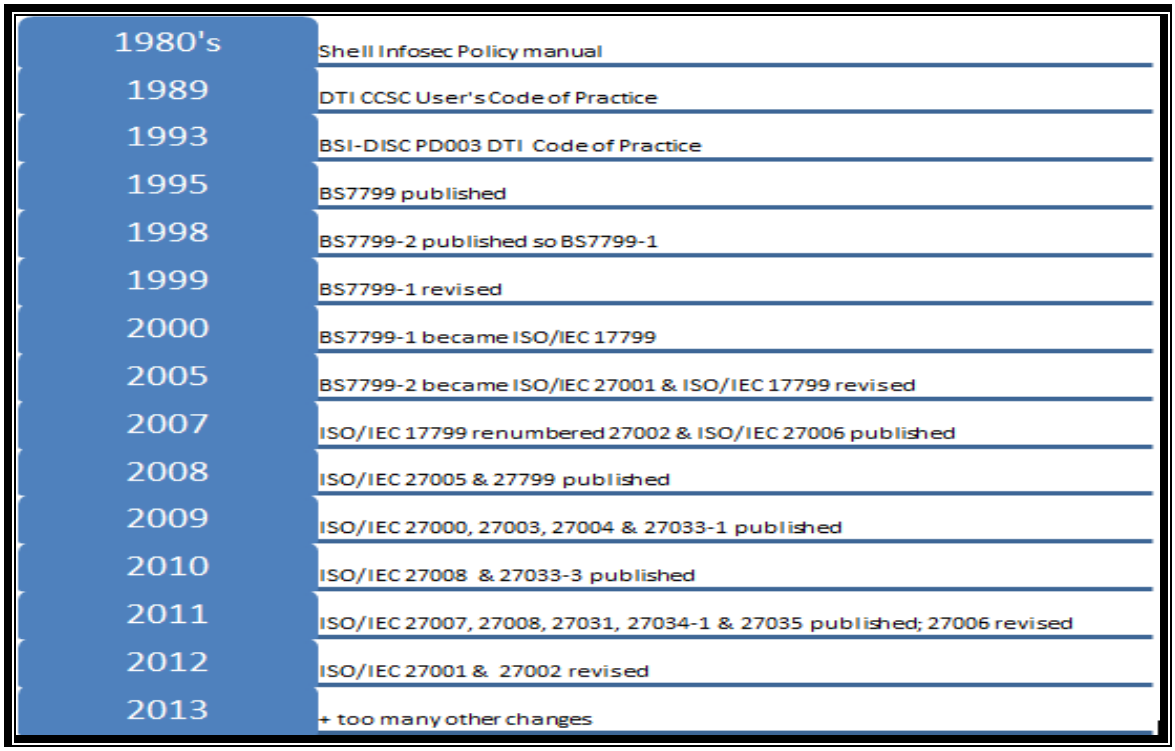


Figure 2.6 ISO/IEC 27000 family of standard timeline (Noticebored, 2017b)

The study focused on the first five standards of the ISO/IEC 27000 family of standards because these are the critical standards for the information security posture of any organisation (Kearns, 2016; The Government of the Hong Kong Special Administrative Region; 2018). The five standards are described in section 2.6.1.1 - 2.6.1.5. Table 2.3 demonstrates how the five standards are applicable to designing a framework for ISO/IEC 27000 family of standards implementation in Namibia.

Table 2.3 ISO/IEC 27000 family of standards application to the study

ISO/IEC Standards	Application to the study
ISO/IEC 27000	Provided the standard overview and vocabulary which enabled the researcher to understand the basics of the ISO/IEC 27000 family of standards and its application to the security of organisations.
ISO/IEC 27001	Specified the Information security management system requirements which assisted the researcher to identify the controls domains for Namibia.
ISO/IEC 27002	Provide detailed guidelines for the design of a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia.
ISO/IEC 27003	This standard is recommended as guidance for the requirements specified in ISO/IEC 27001 for implementation.
ISO/IEC 27004	This standard is recommended for the information security framework audit. To have an effective national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia, the framework needs to be regularly reviewed.

According to DCC (2015), implementing the ISO 27000 family of standards can bring the benefits to an organisation as listed:

- ✓ Information security issues, and how to mitigate associated risks, will be identified, managed, monitored and improved in a planned manner
- ✓ Appropriate processes and procedures for information security management will be defined, documented and embedded in practice

- ✓ Demonstration of organisational commitment to information security will ensure adequate allocation of resources, identification of roles and responsibilities and appropriate training
- ✓ Data will be protected against unauthorised access, demonstrating its authoritative nature, while authorised users will have access to data when they require it
- ✓ Continuity of an organisation's business will be effectively managed, improving its profile and increasing opportunities
- ✓ Intellectual property rights can be protected
- ✓ Independent verification of compliance with the standard can ensure that an organisation has not been negligent regarding appropriate laws on the privacy of personal information

The next sections (2.6.1.1 – 2.6.1.5) will discuss the first five standards of the ISO/IEC 27000 family of standards in detail.

2.6.1.1 ISO/IEC 27000

ISO/IEC 27000 is the first standard of the ISO/IEC 27000 family of standards and it provides the ISMS overview and vocabulary and it is suitable for any organisation (ISO, 2016). The ISO/IEC 27000 standard has different sections to provide the ISMS overview and vocabulary (International Organisation for Standardization, 2018):

- ✓ Introduction
- ✓ Scope
- ✓ Normative references
- ✓ Terms and definitions
- ✓ Information security management systems
- ✓ ISMS family of standards

ISO/IEC 27000 standard sections will guide the information security experts on the ISMS overview and vocabulary when implementing the national adoption policy framework for ISO/IEC 27000 standards.

2.6.1.2 ISO/IEC 27001

All organisations store data that should be protected from unauthorized access, in sectors such financial services, health, public and information technology sectors. ISO/IEC 27001 is valuable because information protection is critical (BSI, 2009). The standard uses a top down risk-based approach and it is technology-neutral (Rouse, 2009).

ISO/IEC 27001 provides a common framework and specifies security controls, with control objectives and controls that any organisation can implement based on their needs to help organisations to identify, manage, and quantify their information security risks (BSI, 2009). This is provided in different sections of the ISO/IEC 27001 standard as listed in the next section.

ISO/IEC 27001 Standard Structure

The ISO/IEC 27001 framework consists of the following sections (International Organisation for Standardization/International Electrotechnical Commission (ISO/IEC), 2013b):

- ✓ Chapter 0: Introduction
- ✓ Chapter 1: Scope
- ✓ Chapter 2: Normative references
- ✓ Chapter 3: Terms and conditions
- ✓ Chapter 4: Context of the organisation
- ✓ Chapter 5: Leadership
- ✓ Chapter 6. Planning
- ✓ Chapter 7. Support
- ✓ Chapter 8. Operations
- ✓ Chapter 9. Performance evaluation
- ✓ Chapter 10. Improvement
- ✓ Annex A: Reference control objectives and controls

The different sections will guide experts from different organisations when implementing the national adoption policy framework for ISO/IEC 27000 standards.

The ISO/IEC 27001 security standards use the plan-do-check-act (PDCA) cycle to establish, implement, operate, monitor, review, and maintain a continuous improvement approach to manage its ISMS (Charu, 2011; Gillies, 2011).

Table 2.4 presents the different ISO/IEC 27001 requirements for each PDCA cycle stage according to Fedco (2015).

Table 2.4 ISO/IEC 27001 requirements for each PDCA cycle stage

PDCA Cycle	ISO/IEC 27001 Requirements
PLAN	Chapter 4. Context of the organisation
	Chapter 5. Leadership
	Chapter 6. Planning
	Chapter 7. Support
DO	Chapter 8. Operations
CHECK	Chapter 9. Performance Evaluation
ACT	Chapter 10. Improvement

The study focused on the PLAN stage of the PDCA cycle and the different ISO/IEC 27001 requirements under the PLAN stage. This is discussed under section 5.5.

ISO/IEC 27001 has 14 control domains, 35 control objectives and 114 controls under Annex A. Below is a list of control domains and the number of controls under each control domain of the ISO/IEC 27001 (ISO/IEC, 2013b):

- ✓ A5 Information security policies - 2 controls
- ✓ A6 Organisation of information security - 7 controls
- ✓ A7 Human resource security - 6 controls
- ✓ A8 Asset management - 10 controls
- ✓ A9 Access control - 13 controls
- ✓ A10 Cryptography - 2 controls
- ✓ A11 Physical and environmental security - 15 controls
- ✓ A12 Operations security - 14 controls
- ✓ A13 Communications security - 7 controls
- ✓ A14 System acquisition, development and maintenance - 13 controls
- ✓ A15 Supplier relationships - 5 controls
- ✓ A16 Information security incident management - 7 controls
- ✓ A17 Information security aspects of business continuity management - 4 controls
- ✓ A18 Compliance - 8 controls

Of the 14 ISO/EIC 27001 control domains, 11 were used for this study namely: information security policy; compliance; information security aspects of business continuity management; communication security; operations security; cryptography; access control; asset management; human resource security; organisation of information security and information security incident management, and they are discussed in section 5.4.2.1.

2.6.1.3 ISO/IEC 27002

ISO/IEC 27002 standard provides detailed guidance on the controls under Annex A of ISO/IEC 27001 as presented in the previous section (Lachapelle & Mustafë, 2016). ISO/IEC 27002 is the Code of Practice for Information Security Control (Lachapelle & Mustafë, 2016). The ISO/IEC 27002 sections are used to guide the ISO/IEC 27001 controls and they are presented in the next sub-section.

ISO/IEC 27002 Standard Structure

The standard has the following sections (International Organisation for Standardization/International Electrotechnical Commission (ISO/IEC), 2013a)):

- ✓ Scope
- ✓ Normative references
- ✓ Terms of this standard
- ✓ Structure of the standard
- ✓ 14 Clauses

ISO/IEC 27002 has 14 clauses which are equivalent to the 14 control domains in ISO/IEC 27001. ISO/IEC 27002 collectively has 35 control objectives and 114 controls. Clauses are structured in this way (ISO/IEC, 2013a):

- ✓ a control objective stating what is to be achieved
- ✓ one or more controls that can be applied to achieve the control objective
    - ➢ Control
    - ➢ Implementation guidance
    - ➢ Other information

2.6.1.4 ISO/IEC 27003

ISO/IEC 27003 provides guidance for the requirements specified in ISO/IEC 27001 for the implementation of the ISMS (ItGovernance, 2017). The standard follows the same structure as ISO/IEC 27001, expanding clause by clause and the structure is (Noticebored, 2017a):

- ✓ Introduction
- ✓ 1 Scope
- ✓ 2 Normative references
- ✓ 3 Terms and definitions
- ✓ 4 Context of the organisation
- ✓ 5 Leadership

- ✓ 6 Planning
- ✓ 7 Support
- ✓ 8 Operation
- ✓ 9 Performance evaluation
- ✓ 10 Improvement
- ✓ Annex - Policy framework

2.6.1.5 ISO/IEC 27004

ISO/IEC 27004 provides guidelines to monitor, measure, analyse and evaluate the ISMS performance and effectiveness to meet the requirements of the ISO/IEC 27001 (Kelechava, 2017; ISO, n.d.-b). The standard has the following sections that are used to provide guidelines to the ISO/IEC 27001 requirements (ISO/IEC, 2016):

- ✓ Scope
- ✓ Normative references
- ✓ Terms and conditions
- ✓ Structure and overview
- ✓ Rationale
- ✓ Characteristics
- ✓ Types of measures
- ✓ Processes
- ✓ Annex A (informative) An information security measurement model
- ✓ Annex B (informative) Measurement construct examples
- ✓ Annex C (informative) An example of free-text form measurement construction

The first five standards of ISO/IEC 27000 family of standards presented will be used for the design, implementation, audit and maintenance of the national adoption policy framework for ISO/IEC 27000 standards. The standards sections listed will guide the information security experts when implementing the national adoption policy framework for ISO/IEC 27000 standards.

The ISO/IEC 27001 is the most adopted and used ISMS, and it is used globally by 163 countries (Shojaie, Federrath & Saberi, 2015; Susanto, Almunawar & Tuan, 2011). Despite its extensive use, the ISO/IEC 27000 family of standards can have several factors affecting its adoption in organisations. Several authors list these factors as (AbuSaad, Saeed, Alghathbar, Khan, 2011; Kiilu & Nzuki, 2015; Song, 2017):

- ✓ Information Security Awareness Training
- ✓ Identifying the organisation's assets
- ✓ Weak team experience
- ✓ Deployment of the wrong employees
- ✓ Resistance to change
- ✓ Unclear understanding of the standard
- ✓ Lack of top management involvement
- ✓ Lack of employee discipline on information security
- ✓ External influences (security breaches, technology changes and regulatory forces)
- ✓ Organisational information security culture
- ✓ Inadequate budget
- ✓ Poor enforcement of regulations, policies and procedures
- ✓ Improper documentation of policies and other information security documents

Even though there are different factors as listed above affecting the adoption of ISMS in organisations, organisations have successfully adopted the ISMS standards. Examples of organisations in Africa that successfully adopted the ISMS are:

- ✓ Central Bank of Nigeria as the regulator of the Financial Services Industry in Nigeria implemented the ISO/IEC 27001, and the systematic management framework was implemented to protect its information assets. The implementation process was a success because of top management commitment and support, staff cooperation and participation (BSI, n.d.-a).

- ✓ Nigeria Social Insurance Trust Fund (NSITF) implemented the ISO 27001, a globally recognised standard, to comply with regulatory and legal requirements in order to protect their information assets and minimise their reputation risk. The implementation process was a success because they used a reputable consultant, the senior management formed an information security forum and there was an appointment of ISO champions in all departments (BSI, n.d.-c).

- ✓ Gulf Insurance Group K.S.C. (GIG), a company in Kuwait adopted the ISMS to maintain the confidentiality, integrity and availability of information and assets. The implementation process was successful because they created an ISMS forum for communicating ISMS activities, conducted a GAP analysis to understand the current information security posture, training the implementation team and engaging consultants (BSI, n.d.-b).

The next section will discuss steps used to implement the ISMS.

2.7 ISMS Implementation

Implementation is the action carried out or the practice of a plan, a method, or any design, idea, model, specification, standard or policy for something to actually happen (Rouse, 2015). ISMS implementation is the identification and management of information security risks offered through a practical and pragmatic framework depending on the needs (organisation's size, the information security threats it faces and the measures in place etc.) and the organisation's objectives (Irwin, 2017; Queensland Government, 2017). When implementing an ISMS, the following steps exist as listed in table 2.5. Steps from different authors are illustrated, authors have some steps that are similar and some steps that are different. The once suitable for this study are selected from the different authors.

Table 2.5 ISMS Implementation Steps

Authors	ISMS Implementation Steps
Irwin (2017)	✓ Conduct a gap analysis ✓ Scope the ISMS ✓ Develop your information security policy ✓ Conduct a risk assessment ✓ Select your controls ✓ Create a Statement of Applicability (SoA) ✓ Set up a risk treatment plan (RTP) ✓ Create your documentation ✓ Roll out a staff awareness programme ✓ Conduct regular testing ✓ Conduct management reviews ✓ Choose your certification body ✓ Gain accredited certification ✓ Manage and review your ISMS
Kosutic (2018)	✓ Obtain management support ✓ Treat it as a project ✓ Define the scope ✓ Write an ISMS Policy ✓ Define the Risk Assessment methodology ✓ Perform the risk assessment and risk treatment ✓ Write the Statement of Applicability ✓ Write the Risk Treatment Plan ✓ Define how to measure the effectiveness of controls ✓ Implement the controls and mandatory procedures ✓ Implement training and awareness programmes ✓ Operate the ISMS ✓ Monitor the ISMS ✓ Internal audit ✓ Management review

Authors	ISMS Implementation Steps
	✓ Corrective and preventive actions
Kadam (2003)	**Plan (establish the ISMS)** ✓ Establish the importance of Information Security in Business ✓ Define the Scope for ISMS ✓ Define the Security Policy ✓ Establish the Security Organization Structure ✓ Identify and Classify the Assets ✓ Identify and Assess the Risks ✓ Plan for Risk Management **Do (Implement and operate the ISMS)** ✓ Implement Risk Mitigation strategy ✓ Write the Statement of Applicability ✓ Train the staff and create Security Awareness **Check (Monitor and review ISMS)** ✓ Monitor and Review the ISMS performance **Act (Maintain and improve the ISMS)** ✓ Maintain the ISMS and ensure continual Improvement

The standard from the ISO/IEC 27000 family of standards used for the ISMS implementation is the ISO/IEC 27001, which uses the PDCA cycle to establish, implement, operate, monitor, review, and maintain the ISMS (Charu, 2011; Gillies, 2011; Irwin, 2017). Since ISO/IEC 27001 uses PDCA cycle for continuous improvement approach to manage its ISMS, the implementation steps in table 2.5 were divided into the PDCA cycle stages as shown in table 2.6.

Table 2.6 ISMS Implementation Steps divided into PDCA cycle

Kadam (2003)	Irwin (2017)	Kosutic (2018)
Plan (establish the ISMS) ✓ Establish the importance of Information Security in Business ✓ Define the Scope for ISMS ✓ Define the Security Policy ✓ Establish the Security Organisation Structure ✓ Identify and Classify the Assets ✓ Identify and Assess the Risks ✓ Plan for Risk Management	✓ Conduct a gap analysis ✓ Scope the ISMS ✓ Develop your information security policy ✓ Create your documentation ✓ Conduct a risk assessment ✓ Select your controls	✓ Obtain management support ✓ Treat it as a project ✓ Define the scope ✓ Write an ISMS Policy ✓ Define the Risk Assessment methodology ✓ Define how to measure the effectiveness of controls ✓ Perform the risk assessment & risk treatment
Do (Implement and operate the ISMS) ✓ Implement Risk Mitigation strategy ✓ Write the Statement of Applicability ✓ Train the staff and create Security Awareness	✓ Create a Statement of Applicability (SoA) ✓ Set up a risk treatment plan (RTP) ✓ Roll out a staff awareness programme	✓ Implement the controls & mandatory procedures ✓ Write the Statement of Applicability ✓ Write the Risk Treatment Plan ✓ Implement training and awareness programs ✓ Operate the ISMS
Check (Monitor and review ISMS) ✓ Monitor and Review the ISMS	✓ Conduct regular testing	✓ Monitor the ISMS ✓ Internal audit

Kadam (2003)	Irwin (2017)	Kosutic (2018)
performance	✓ Conduct management reviews ✓ Choose your certification body ✓ Gain accredited certification	
Act (Maintain and improve the ISMS) Maintain the ISMS and ensure continual Improvement	Manage and review your ISMS	✓ Management review ✓ Corrective and preventive actions

As mentioned earlier, the study focused on the Plan stage of the PDCA cycle hence the ISMS implementation steps under the Plan stage will be discussed. The ISMS implementation steps from the three authors in table 2.5 and 2.6 were combined for this study and they are presented in the next sections. Each author list steps that are missing in another author's list hence the steps were combined and if the steps are similar one was selected. The steps were combined to ensure that all the steps are used for a thorough implementation process. These steps are recommended when implementing the national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia:

- ✓ Establish the importance of Information Security in Business
- ✓ Conduct a gap analysis
- ✓ Define the scope for ISMS
- ✓ Establish the Security Organization Structure
- ✓ Define the Information Security Policy
- ✓ Identify and Classify the Assets
- ✓ Select your controls
- ✓ Create your documentation
- ✓ Obtain management support
- ✓ Treat it as a project
- ✓ Define how to measure the effectiveness of controls

- ✓ Identify and assess the risks
- ✓ Plan and define the Risk Assessment and Management methodology

Four steps were used to design the theoretical framework as this are the basic steps in determining the security posture of an organisation, hence they are described in detail in the sections below:

- ✓ Conduct a gap analysis
- ✓ Define the Information Security Policy
- ✓ Identify and assess the risks
- ✓ Plan and define the Risk Assessment and Management methodology

2.7.1 Conducting a Gap Analysis

Gap analysis is a process which involves benchmarking the organisation's information security current state with the required or target state (Peltier, 2010). The role of a gap analysis in information security is to identify an area that the organisation is not compliant with the information security best practices (e.g. ISO/IEC 27001), where vulnerabilities and risks are lurking and what needs to be done to become compliant (Irwin, 2017; Sell, 2015). This saves the organisation time and money by focusing on areas that are not compliant and promoting the areas that are compliant rather than adopting new ones (Shaw, 2012).

Gap analysis with ISO 27001 involves comparing the standard's clauses and security controls to determine which of those requirements are implemented by the organisation (Gardner, 2017). Gardner (2017) further states that the gap analysis for clauses 4 – 10 of ISO/IEC 27001 is optional but it is recommended and it is mandatory for the 114 security controls in Annex A.

Sell (2015) suggests four steps when performing an information security gap analysis:

- ✓ Step 1: Select an industry standard security framework
- ✓ Step 2: Evaluate people and processes

- ✓ Step 3: Data gathering
- ✓ Step 4: Analysis

Kosutic (n.d.-b) recommends that when performing gap analysis you can indicate YES/NO for the clauses and security controls or use the 5 scale below to determine the extent of ISO 27000 family of standards implementation in organisations.

- ✓ 0 – requirement not implemented nor planned
- ✓ 1 – requirement is planned but not implemented
- ✓ 2 – requirement is implemented only partially, so that full effects cannot be expected
- ✓ 3 – requirement is implemented, but measurement, review and improvement are not performed
- ✓ 4 – requirement is implemented and measurement, review and improvement are performed regularly

As mentioned above, performing a gap analysis is done by comparing ISO/IEC 27001 clauses and security controls or determining the extent of ISO 27000 family of standards implementation in organisations. The research project aimed to determine the gap analysis (implementation extent) of the standards not the standard's clauses and security controls. The gap analysis was to determine if the standard is at all implemented in Namibian organisations and not which standards' clause and controls are the organisations implementing due to the study's time limit. The gap analysis scale can be used to determine the ISO/IEC 27001 standard implementation extent in Namibian organisations. The outcome of the gap analysis can be used as the input to the design of the national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia and the theoretical framework as discussed in section 2.8.

The next section discusses the information security policy and its role in ensuring organisational security.

2.7.2 Define the Information Security Policy

An information security policy is described as a set of rules and procedures that reflects the organisation's security objectives, to ensure that all users abide by the rules of the organisation's IT assets and resources (Bayuk, 2009; Kostadinov, 2014; Palo Alto Networks, 2017).

Different authors listed in table 2.7 specify the structure that an information security policy should contain.

Table 2.7 Information Security Policy Structure

Authors	Information Security Policy Structure
Bayuk (2009)	1 Scope 2 Information classification 3 Management goals 4 Context 5 Supporting documents 6 Specific instructions 7 Responsibilities 8 Consequences
SANS Institute (2007)	1 Introduction 2 Purpose 3 Scope 4 Roles and Responsibilities 5 Sanctions and Violations 6 Revisions and Updating Schedule 7 Contact information 8 Definitions/Glossary 9 Acronyms
Kostadinov (2014)	1 Purpose 2 Scope 3 Information security objectives

Authors	Information Security Policy Structure
	4 Authority & Access Control Policy 5 Classification of Data 6 Data Support & Operations 7 Security Awareness Sessions 8 Responsibilities, Rights and Duties of Personnel 9 Reference to Relevant Legislation
Heriot-Watt University (2013)	1 Introduction 2 Purpose 3 Objectives 4 Scope 5 Lines of responsibility 6 Monitoring and Evaluation 7 Implementation 8 Related Policies, procedures and further reference 9 Definitions 10 Further help and advice 11 Policy Version and History

The following information security policy structures were selected from table 2.7 based on the theoretical framework components, namely introduction, purpose, objectives, scope, responsibilities, rights and duties of personnel, monitoring and evaluation, and specific instructions were used to explain the components of the national adoption policy framework for ISO/IEC 27000 standards implementation in organisations and nations such as Namibia (as discussed in section 5.7.1). The study will design a framework implementation guideline for the adoption of a policy framework for ISO/IEC 27000 standards implementation in general, which consist of the following components: ISO/IEC 27001 information security controls (discussed in section 2.6.1.2), ISMS pillars (discussed in section 2.2.3), and information security pillars (discussed in section 2.8.1). Based on literature surveyed, the information security pillars are confidentiality, integrity, availability, non-repudiation and authentication (United State Naval Academy, n.d.). The information security pillars are part of the framework implementation guidelines and they are discussed in section 5.4.2.3.

A successful policy starts with understanding the information security risks. The next section discusses the information security risk.

2.7.3 Information Security Risk

Information security risk is described as intentional or unintentional events that can cause damage to a process or related information (Elky, 2006). An organisation can have the right technology, policies, procedures and tools but if their employees are not properly trained they might engage in risky behaviours that can put an organisation at risk (Cisco, 2014; Ford, 2013). Cisco (2014) states that the following employee behaviours can put the organisation at risk, namely unauthorized application use, misuse of corporate computers, unauthorized physical and network access, remote worker security and misuse of passwords.

Biscoe (2017b) presents the information security risks as social engineering, disclosure of information or passwords, access to the network by unauthorised persons, errors in maintenance, loss of electricity, human or natural disasters, malfunction of equipment, destruction of records, theft of hardware and fire. Hau (2013) also presents information security risks as unauthorized disclosure of information, disruption of computer services, loss of productivity, financial loss, legal implications and organisational blackmail.

All information security risks mentioned by Biscoe (2017b), Cisco (2014) and Hau (2013) can apply to Namibian organisations if proper processes like the national adoption policy framework for ISO/IEC 27000 standards are not implemented. To review and confirm security controls, ISO/IEC 27001 is specific that a risk management process should be used (Biscoe, 2017b). The two steps from the ISMS implementation steps that deal with information security risks are discussed next.

2.7.3.1 Identify and Assess the Risks

Risk identification is the process of identifying negative and positive threats, risks and vulnerabilities that impact information security controls (Irwin, 2017; Kosutic, 2018; Sharma, 2012). Risk assessment is the process of gauging the consequence of the threats, risks and vulnerabilities qualitatively and quantitatively (Irwin, 2017; Kosutic, 2018; Sharma, 2012). Risk identification tells you the risk that will affect the information security controls and risk assessment tells you how the risk will affect the information security controls (Irwin, 2017; Kosutic, 2018; Sharma, 2012).

2.7.3.2 Definition of the Risk Assessment and Management Methodology

Kosutic (2018) states that risk assessment deals with defining the acceptable level of risk and defining the rules for identifying the assets, vulnerabilities, threats and impacts.

Risk management focusses on identifying, quantifying, and managing the cost benefit analysis of different options used to handle risk, for example transferring the risk, risk avoidance, risk acceptance and risk reduction (Financial Times, n.d.; Kadam, 2003).

2.8 Theoretical Framework

A theoretical framework is a collection of interrelated concepts; it provides a general representation of relationships between concepts in a given phenomenon (Borgatti, 1999; Regoniel, 2010). Additionally, Regoniel (2010) posits that a theoretical framework dwells on time tested theories that represent the findings of different investigations on how phenomena occur. A theoretical framework should be logical and there are no fixed rules on how it should be structured (Vinz, 2017).

Vinz (2017) mentions the steps for designing a theoretical framework as:

- ✓ Select key concepts
    - ➢ Sample problem statement and research questions
    - ➢ Problem
    - ➢ Objective

- Research question

- ✓ Define and evaluate relevant concepts, theories, and models
- ✓ Consider adding other elements to your theoretical framework

The steps for developing the theoretical framework are discussed in detail in section 5.4.

2.9 Summary

Namibia is rated as an insecure nation and the absence of best practices adoption guidelines is a security risk for the nation. For effective information security governance and implantation, Namibia needs to have a strategy to implement known models and frameworks for information security. The chapter briefly discussed the different information security layers and the selected layer for this study is the information security layer which consists of the following components: information security management, computer and data security, and network security. The information security management component of the information security layer was the focal point for this study and it has these components: organisation, people, process and technology. The organisation component for this study was the different organisations in Namibia and preliminary interviews with selected stakeholders from these organisations were conducted in 2015 and they revealed that there is a lack/no implementation of the ISO/IEC 27000 family of standards in organisations. The people's component focuses on everyone in an organisation who needs information security awareness and the information security specialists.

To implement information security best practices, information security specialists need to be certified and trained in information security qualifications and ISO/IEC 27001 certification is one such qualification. The ISO survey depicted that no one in Namibia was certified in ISO/IEC 27001.

The technology component represents the tools, applications and infrastructure that make the process component more efficient. And finally, the process component compared the ISMS and the different information security governance standards and the ISMS was selected for this study. ISO/IEC 27000 family of standards is a requirement for creating ISMS and it was discussed in detail for the purpose of this study. ISO/IEC 27000 family of standards was found to be suitable for Namibia as it encourages the implementation of the lack/no implementation of the ISO/IEC 27000 family of standards in organisations and the certification of information security specialists in ISO/IEC 27001. Methods of risk analysis, solution design and security compliance such as the gap analysis, the theoretical framework, information security policy, ISMS pillars, information security pillars and the information security risk were also discussed in this chapter. These provide the necessary tools for developing an adoption strategy for Namibia.

The next chapter discusses the methodologies used for this study.

Chapter 3 – Methodology

3.1 Introduction

Chapter two discussed literature relevant to the study and specified what the research will achieve. The purpose of the present chapter is to discuss the different methodologies that were used to collect and analyse data to answer the research questions and meet the research objectives. Research methods choice involves the selection of data collection techniques and data analysis procedures, namely quantitative and qualitative (Saunders, Philip, & Thornhill, 2009). Quantitative research generates numerical data by quantifying attitudes, opinions, behaviours, and other defined variables using structured data collection methods (Wyse, 2011). Qualitative research generates words rather than numbers as data for analysis to uncover trends and to gain an understanding of underlying reasons, opinions and motivation by using unstructured or semi-structured data collection methods (Brikci & Green, 2007; Wyse, 2011).

Saunders et al. (2009) describe three methods used when selecting data collection techniques and the analysis of procedures to answer the research question:

Mono methods – use a single data collection technique and corresponding analysis procedures
Multi methods – use more than one data collection technique and analysis procedures, either multiple quantitative or qualitative methods but not both
Mixed methods – use both quantitative and qualitative data collection techniques and analysis procedures, either at the same time or one after the other without combining the methods.

A multi method qualitative research was used in this case to help us understand the phenomenon and answer the research questions.

This section introduced the purpose of this chapter and research methods choice. The selected method was presented. The next sections will discuss the following topics: research process, research design, research quality, the ethical considerations for the project and a chapter summary.

3.2 Research Process

The research process defines different but linked methods that are used to undertake the research project (Saunders, Philip, & Thornhill, 2009). Saunders et al. (2009) mention the different research processes under their research onion as research approach, research strategies, research choices, time horizons and techniques and procedures. The different research processes and how they apply to the research project are discussed in the following sections.

3.2.1 Research Approach

The research approach is the reciprocal relationship between theory and research on how they structure and inform each other, with steps of the detailed method of data collection, analysis and interpretation (Blackstone, 2016; Sudeshna & Shruti, 2016). Two research approaches exist, namely the inductive approach and the deductive approach.

3.2.1.1 Inductive Approach

In an inductive approach, a researcher collects data that is relevant to their area of interest and then looks for patterns in the data, working to develop a theory that can explain those patterns (Blackstone, 2016).

The inductive approach follows a bottom-up approach process and uses mostly qualitative methods of data collection and data analysis (Dudovskiy, 2017). Figure 3.1 outlines the different steps used in an inductive approach:

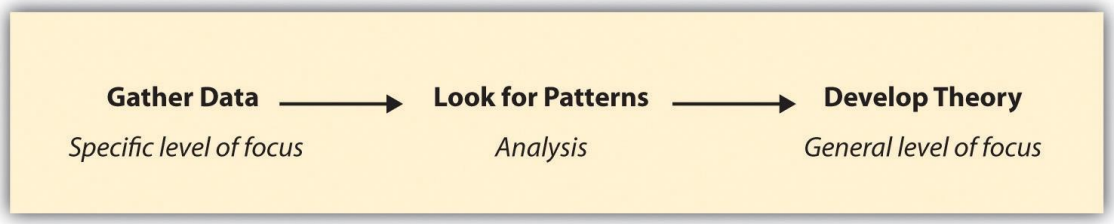


Figure 3.1 Inductive approach research steps (Blackstone, 2016)

3.2.1.2 Deductive Approach

In a deductive approach the researcher studies the literatures by others that are related to their area of interest and tests the hypotheses from those literatures to determine whether the hypothesis is valid or not (Blackstone, 2016). The deductive approach follows a top-down approach process and uses quantitative methods of data collection and data analysis (Dudovskiy, 2017). Figure 3.2 outlines the different steps used in a deductive approach:

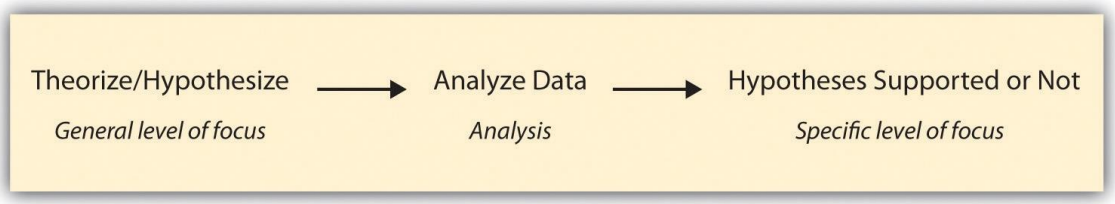


Figure 3.2 Deductive approach research steps (Blackstone, 2016)

The study designed a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia. This was achieved by collecting data using preliminary interviews with selected stakeholders to perform a gap analysis of ISO/IEC 27000 family of standards in Namibian organisations.

A theoretical framework was designed from the gap analysis results and literatures. The theoretical framework was evaluated by experts from selected organisations and the results were analysed to validate the effectiveness of the framework. A national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia was designed from the analysed data. The processes executed to design the national adoption policy framework for ISO/IEC 27000 standards implementation justify that an inductive research approach was the appropriate approach for the study.

3.2.2 Research Strategies

The research strategy is a procedure that is used to answer research questions and meet objectives (Saunders et al., 2009). The different research strategies are discussed in table 3.1.

Table 3.1 Research Strategies (Saunders et al., 2009)

Research Strategies	Description
Experiment	Involves the definition of a theoretical hypothesis; the selection of samples of individuals from known populations; the allocation of samples to different experimental conditions; the introduction of planned change on one or more of the variables; and measurement on a small number of variables and control of other variables.
Survey	Involves the structured collection of data from a sizeable population. Although the term 'survey' is often used to describe the collection of data using questionnaires, it includes other techniques such as structured observation and structured interviews.
Case study	Involves the empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence. Types of case studies: (Oates, 2012, pp. 141 - 143) **Exploratory study** – Used to help a researcher to understand a research problem and define the questions or hypotheses to be used for the study **Descriptive Study** – Detailed analysis of a phenomenon and its context. **Explanatory Study** – Compares what was found in the case to theories from the literature review in order to see whether one theory matches the case.
Action research	Concerned with the management of a change and involving close collaboration between practitioners and researchers. The results

Research Strategies	Description
	flowing from action research should also inform other contexts.
Grounded theory	Theory is developed from data generated by a series of observations or interviews principally involving an inductive approach.
Ethnography	Focuses upon describing and interpreting the social world through firsthand field study.
Archival research	Research strategy that analyses administrative records and documents as principal sources of data because they are products of day-to-day activities.

Since the study sought to understand why there is no adoption of ISO/IEC 27000 family standards to secure electronic information nationally, an in-depth study of the case provided a detailed understanding in context. A case study research strategy with security critical organisations in Namibia was used for this research and a survey research strategy was used to collect data from the different case sites.

3.2.2.1 Case study

An exploratory case study was used for this study with the following organisations: Office of the Prime Minister (OPM), Ministry of Information and Communication Technology (MICT), Communication Regulatory Authority of Namibia (CRAN), Telecom Namibia (TN) and Namibia Institute of Standards (NIS). The OPM is responsible for the strategic plan, co-ordination of cabinet matters and projects/programmes (Office of the Prime Minister, n.d.). MICT is responsible for the development and promotion of ICT growth, and it provide effective information services, promotes constructive dialogue towards socio-economic development and democracy (MICT, n.d.). CRAN controls the operations of telecommunication services and networks, broadcasting services, postal services and the use and allocation of the radio spectrum (CRAN, n.d.). TN which is an Internet Service Provider (ISP), is responsible for providing individuals and other companies access to the Internet and other related services (Rouse, 2006).

NIS is responsible for the promotion of standardisation and quality assurance in the industry, commerce and the public sector in Namibia (ISO, n.d.-c), and these critical organisations are responsible for ensuring secure access of authorised content to citizens.

The six steps below for a case study research by Yin (2009) were adopted for this study:

3.2.2.1.1 Plan

ISO/IEC 27000 family of standards provides Information Security Management System best practices and there is a poor/no implementation of the standard in Namibian organisations. The study investigated the extent to which the ISO/IEC 27000 family of standards is implemented, the challenges of adopting the framework, and then designed an implementation framework which can be used to mitigate information security risks in Namibia.

The study focused on the implementation extent and challenges for ISO 27000, 27001, 27002, 27003 and 27004, as these are the critical standards to the security posture of any organisation to mitigate information security risks and as such the security of the nation. To implement an appropriate framework for Namibia, research questions, objectives and data collection methods in table 3.2 were used for this study.

Table 3.2 Research questions and methods for the implementation of ISO/IEC 27000

Questions	Objectives	Data collection Methods
What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?	Investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia	- Case study - Literature review - Interview
What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?	Investigate the factors affecting the adoption of ISO/IEC 27000 family of standards	- Case study - Literature review - Interview
How can a policy framework be constituted to guide the adoption of	Design a policy framework to guide the adoption of ISO/IEC	- Case study - Literature review

Questions	Objectives	Data collection Methods
ISO/IEC 27000 family of standard into security practice?	27000 security standards in the practice	- Questionnaire - Design science methodology - Design and development stage

3.2.2.1.2 Design

According to Yin (2009), there are two types of case study designs, namely single and multiple case study design, and within the two designs there can be single or multiple units of analysis. The four types of case study design are:

- ✓ Type 1 - single-case (holistic) designs
- ✓ Type 2 - single-case (embedded) designs
- ✓ Type 3 - multiple-case (holistic) designs
- ✓ Type 4 - multiple-case (embedded) designs

Figure 3.3 displays the different case study designs from which a researcher can choose the applicable one to their situation.

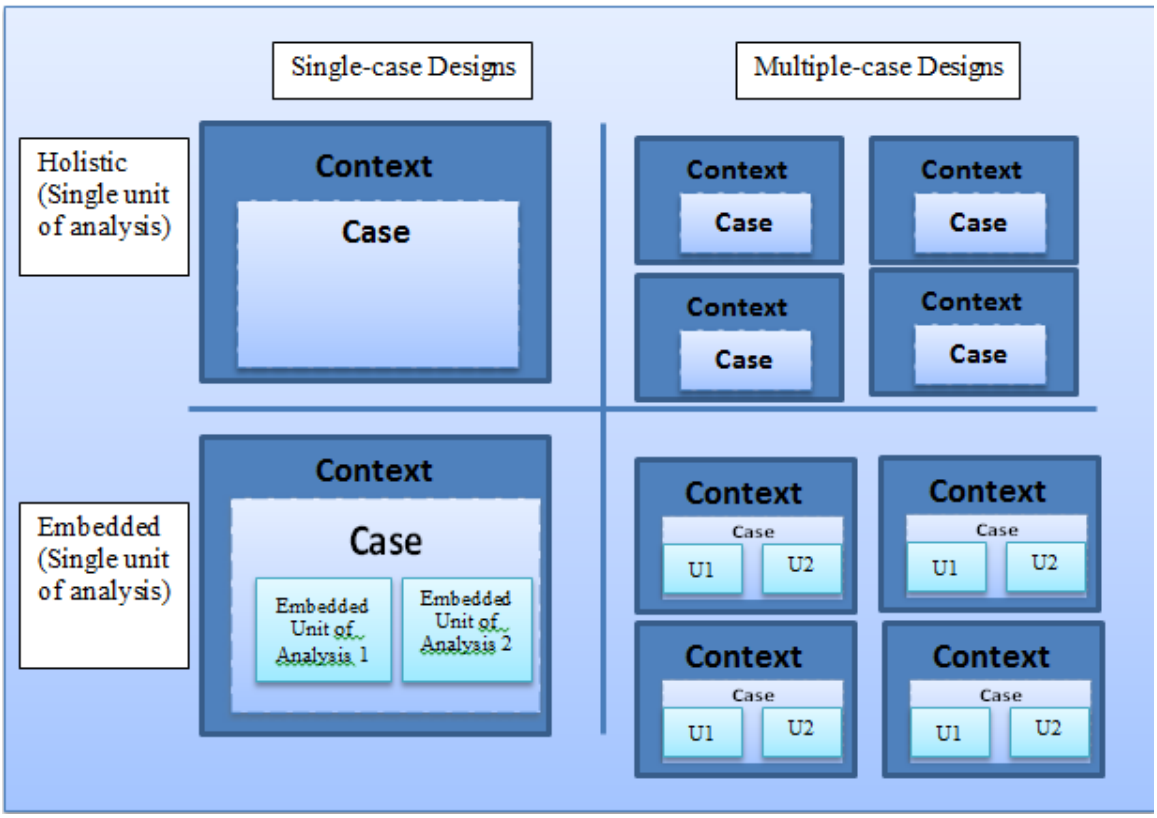


Figure 3.3 Types of case study designs (Yin, 2009)

The study investigated the implementation extent and the factors affecting the adoption of the ISO/IEC 27000 family of standards in Namibian organisations. Type 2 - single-case (embedded) design was used for this study. Different stakeholders in Namibia selected for this research are OPM, MICT, CRAN, TN and NIS.

Collecting data from a sub-group instead of the whole population being studied due to time, money or access to the population is called sampling. According to Saunders et al. (2009), there are two categories of sampling methods, namely probability and non-probability sampling (see table 3.3).

Table 3.3 Sampling methods (Saunders et al., 2009)

Sampling Category	Sampling Methods	How the samples are selected
Non-probability sampling	Convenience sampling	Participants are randomly selected based on ease of availability (p.241)
	Snowball sampling	Involves selecting one or two participants that meet the research criteria, these participants are then used to identify the other participants. (p. 240)
	Purposeful sampling	Participants are selected based on the researcher's judgement on whether they will answer the research question and meet the objectives (p. 237)
	Quota sampling	Participants are divided into specific groups and the selection is entirely non-random (p. 235)
	Typical case sampling	Participants are selected on the basis that they are typical or illustrative to a specific study (p. 240)
	Theoretical sampling	Participants are critically selected based on the basis that they will further the development of concepts and categories and to explore relationships between these to develop a theory (p. 509)
Probability sampling	Simple random sampling	Participants are randomly selected from a sampling frame until a sampling size is obtained (p. 222)
	Systematic random sampling	Participants are selected at regular intervals from a sampling frame using a sampling fraction (p. 226)
	Stratified sampling	Participants are divided into two or more relevant strata based on certain attributes. A simple

Sampling Category	Sampling Methods	How the samples are selected
		random sampling or systematic random sampling is then executed on each of the strata (p.228)
	Cluster sampling	Participants are divided into discrete groups called clusters. Complete lists of clusters are then used as a sampling frame (p. 230)

Purposeful sampling was used to select stakeholders for the research study. The stakeholders were purposefully selected as they could offer rich information about the phenomenon under study. Experts from the industry and academia were selected to evaluate the functionality of the theoretical framework and its components. Convenience sampling was used to select participants for the framework pilot study. The selected participants were Information Security Masters students at the Namibia University of Science and Technology, and several experts from the industry. The researcher is a student at the Namibia University of Science and Technology, and also works in the IT industry, so it was easy to contact the selected participants for the framework pilot study.

Data used for this study to meet the research objectives and to answer the research questions were collected using semi-structured interviews, literature reviews and questionnaire.

3.2.2.1.3 Prepare

Questions for a semi-structured interview were prepared and the researcher conducted interviews with selected stakeholders. Literature reviews were also conducted (see Appendix C for the semi-structured interview questions).

Self-administered online questionnaires with mostly closed ended questions to evaluate the framework and open-ended questions for additional comments was prepared using google forms (see Appendix D for the questionnaire). The questionnaire, also referred to as the evaluation tool was used to evaluate the framework.

A pilot test of the evaluation tool was conducted with Information Security Masters students at the University of Science and Technology and several experts from the industry. A pilot test is the refinement of the final tool provided to gauge the appropriateness of the tool before the final deployment (Yin, 2011, p. 37). A pilot study was conducted to verify the functionality and usability of the evaluation tool. Few amendments were specified during the pilot survey and changes were made before the evaluation tool was sent out to selected stakeholders.

The purpose and benefits of the research were explained to the stakeholders on the questionnaire cover page to make them aware of the project. They were also informed that the data collected would be used for purposes of the project and they would be kept confidential. This ensured consented participation.

3.2.2.1.4 Collect

Data collection is the process of gathering information from a variety of sources to answer a research question (McLaughlin, 2016). Different data collection methods applicable to qualitative studies are listed in table 3.4.

Table 3.4 Data collection methods

Methods	Description
Interviews	A planned method of obtaining information from the interviewee with an agenda that is guided by the researcher. **Types of interviews:** **Structured interviews** – use pre-determined, standardized, identical questions for all interviewees **Semi-structured interviews** – use predetermined questions but the researcher may change the order of the questions and/or add additional questions based on the flow of the interview **Unstructured interview** – interviewees develop their own ideas about the introduced topic and the researcher has less control over the interview (Oates, 2012, pp. 186 -187)

Methods	Description
Questionnaires	Predefined set of questions in a pre-determined order where respondents provide data that can be analysed and interpreted (Oates, 2012, p. 219). According to Oates (2012, p 219), questionnaires are either: **Self-administered** – The respondent completes the questionnaire without the researcher **Researcher administered** – the researcher asks the respondents all questions and writes down the responses. Two types of questions exist for the questionnaire namely open-ended questions and closed ended questions.
Observations	Involves using your senses to pay attention to what people are doing rather than what they report they are doing when questioned. Two observation methods exist: **Overt** – People are aware that they are being observed **Covert** – Researcher conducts the observation without people's awareness (Oates, 2012, p. 202 -204)
Focus Groups	A facilitated group interview with predetermined topics which consist of six to twelve people with similar characteristics or common interests (Evaluation Research Team, 2008)
Ethnographies	Involve gathering and recording data of people or culture, such as how they live, work, their norms of behaviour and how they dress (Oates, 2012, p. 173) Use other data collection methods such as observation, interviews, and surveys (Oates, 2012, p. 176)
Documents	A way of collecting data by reviewing existing hard copy or electronic documents. Documents can be internal or external to an organisation and can include reports, programme logs, performance ratings, funding proposals, meeting minutes, newsletters, and marketing materials (Evaluation Research Team, 2008)
Case Study	Focus on one instance or case to be studied in depth using a variety of data collection methods to obtain detailed insights of the phenomenon being studied. Use of this data collection method is through documents, observation, interviews, ethnography, and surveys (Oates, 2012, p. 141 - 143)

Data collection was triangulated using literature reviews, semi-structured interviews, and questionnaires with stakeholders. The next sections discusses the different data collection methods used for this study and how they were applied.

3.2.2.1.4.1 Interviews

Preliminary semi-structured interviews (Appendix B) were conducted with the stakeholders to address the first and second research objectives (see table 3.3). The purpose was to collect data that were used to answer the research questions on the standards currently used to protect information, the implementation extent of the ISO/IEC family of standards and the factors affecting the adoption of the standards in Namibia.

3.2.2.1.4.2 Literature review

Literatures of topics relevant to this study were collected to help us understand the topic and validate the issues experienced in Namibian organisations. Literature review is a collection of information relevant to the area of research from books, scholarly articles etc. (Shuttleworth, 2009; The Writing Center, 2018). It provides a critical and in-depth evaluation and summary of the research area (Shuttleworth, 2009; The Writing Center, 2018). Literature review was used to support the first and second research objectives.

3.2.2.1.4.3 Questionnaires

A self-administered online questionnaire was used to evaluate the framework to address the third (main) research objective (see Appendix D for the questionnaire). Different literature sources and the outcome of the questionnaires and interviews were used to determine how ISO/IEC 27000 family standards implementation practises that can be constituted in Namibia. This was accomplished by identifying and analysing implementation practices, challenges encountered in the implementation of standards and the evaluation of frameworks. An ISO/IEC 27000 family of standards adoption policy framework for security standards specific to Namibia can be implemented based on these findings and good security practices.

A link to the self-administered online questionnaire was sent out to the different stakeholders to evaluate the framework (see section 5.6.2 for the results and discussions).

3.2.2.1.5 Analyse

Data collected from the interviews and questionnaires were analysed using the content analysis technique to come up with findings and a meaning for the findings.

Qualitative data analysis is the finding of relationships and themes from the collected data by interpreting and examining the data for the final outcome (Oates, 2012, p. 38). Table 3.5 presents different qualitative methods that could be applied to this study.

Table 3.5 Data analysis methods

Analysis Method	Definition
Content Analysis	An inductive and iterative process that looks at data from different angles by identifying keys, similarities and differences in the text that helps to understand and interpret the raw data (Maree, 2007, p. 101).
Narrative Analysis	Involves the analysis of data collected from participants in the form of stories that are either from a personal experience or historical narratives. The researcher keeps track of the sequences, chronology, stories or processes in the data to understand and interpret the raw data (Maree, 2007, p. 103).
Discourse Analysis	Analysis of the meaning of the spoken and written word to reveal the discursive sources of power, dominance, inequality and bias within specific social, economic, political and historical contexts (Maree, 2007, p. 102).
Hermeneutics	Suggests a way of understanding textual data from documents, transcripts etc. where by the researcher reconstructs the initial intension of the author (Maree, 2007, p. 59 & 101).
Thematic Analysis	Involves identifying themes or patterns, coding and classifying textual

Analysis Method	Definition
	data and interpreting the subsequent thematic structures by seeking commonalties, relationships, overarching patterns, theoretical constructs, or explanatory principles (Lapadat, 2010).

Content analysis was used for this study to come up with meaningful interpretations of the questionnaires and interviews. The six generic steps listed below from Creswell (2003) were applied for this research study:

- ✓ Organize and prepare the data for analysis
- ✓ Read through all the data
- ✓ Begin detailed analysis with a coding process
- ✓ Use the coding process to generate a description of the setting or people as well as categories or themes for analysis
- ✓ Advance how the description and themes will be represented in the qualitative narrative
- ✓ A final step in data analysis involves making an interpretation or meaning of the data

The theory established from the collected data was used to develop a security standard adoption policy framework for Namibia. The process is detailed in section 3.3.

3.2.2.1.6 Share

A thesis report with the study overview, purpose, research objectives, research questions, literature review specific to the study, methodologies used to answer the research questions, findings and recommendation was prepared by the researcher and submitted for grading. The report also includes the ISO/IEC 27000 national adoption framework specific to Namibia which will be distributed to stakeholders.

3.2.3 Time Horizons

This is the period it takes to complete the research, either at a particular time or over a given period, independent of the research strategy used (Saunders et al, 2009). There exist two time horizons, namely longitudinal and cross sectional time horizons.

In a longitudinal study the data are collected from the same individuals for the same subjects repeatedly over a period of time (Rouse, 2013).

In a cross sectional study, data are collected for a specific time frame (UK Essays, 2015). A cross sectional time horizon was used for this research project. Academic research projects are completed within a specific time frame and this research project was not an exception.

3.3 Research Design- Design Science Research Strategy Overview

This section focuses on the design science research approach which was used to design the framework. Design science research (DSR) involves the creation of new knowledge through design of new artefacts and analysis of the use and/or performance of such artefacts (Vaishnavi, Kuechler & Petter, 2017). The artefacts designed for this study is a framework that can be used by Namibian organisations for the implementation of the ISO/IEC 27000 family of standards to mitigate information security risk.

3.3.1 Design Science Research Methodologies

A method is a set of steps used to perform a task and it can be used as an input to a model (March & Smith, 1995). In this section different options for applying the methodologies are presented based on different authors. Different authors interpret and apply the design science research methodologies differently and they are discussed next.

According to Johannesson and Perjons (2014), design science research consists of five steps that are used when designing the artefact:

1. Explicate the Problem - Investigate and analyse the identified problem to determine whether the problem is relevant to the research
2. Define Requirements - Plan a solution for the explicated problem in the form of an artefact and define the requirements
3. Design and Develop Artefact – Come up with an artefact that addresses the problem and fulfils the requirements
4. Demonstrate Artefact - Show the artefact in an illustrative or real-life case
5. Evaluate Artefact - Determine whether the artefact fulfilled the requirements and that the problem could be solved to a certain level

The five steps are shown in figure 3.4 with the input and output from each step.

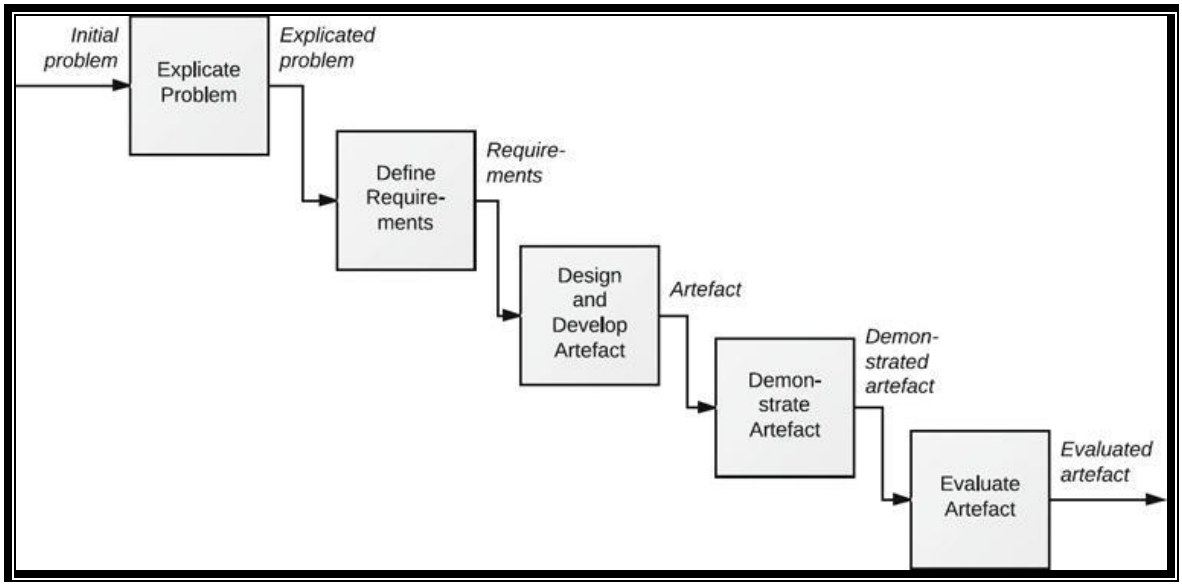


Figure 3.4 Method framework for design science research (Johannesson & Perjons, 2014)

Another method is from Hevner (2007), who states that design science research is based on three cycles namely the relevance cycle, design cycle and rigor cycle. The three cycles are discussed below:

- ✓ The relevance cycle is responsible for gathering requirements, presenting the artefacts into the field, testing and defining criteria for the evaluation of the research results.
- ✓ The design cycle is where the hard work of DSR happens and it is in the middle of the relevance cycle and the rigor cycle as shown in figure 3.5. The design cycle gets the requirement input from the relevance cycle and the methods, design and evaluation theories from the rigor cycle.
- ✓ The rigor cycle is responsible for the knowledge base, it is where the researchers experience and expertise informs the research project

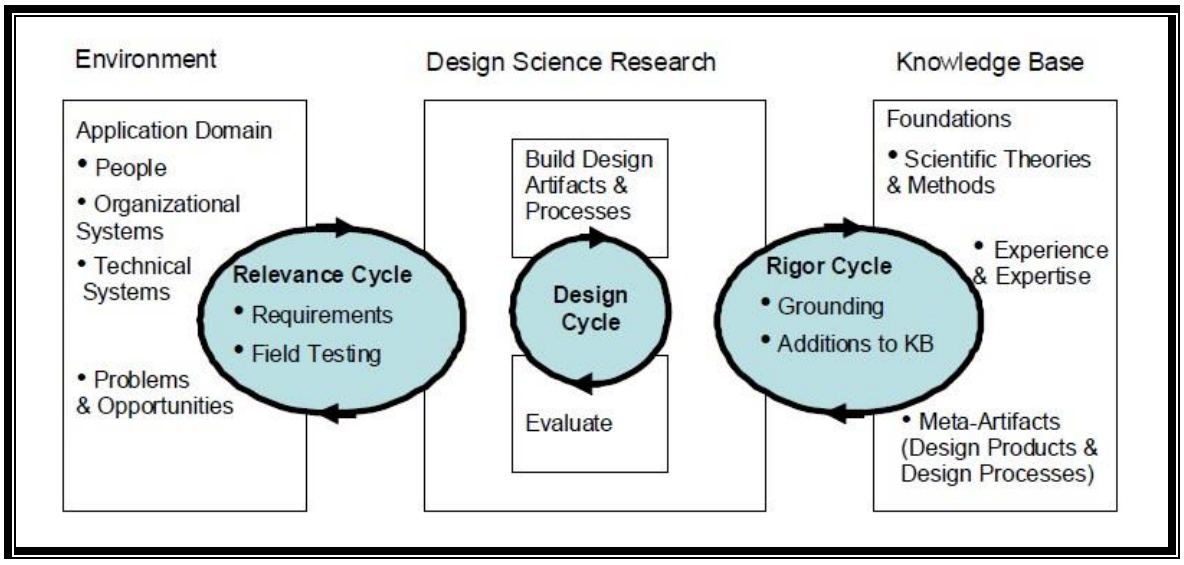


Figure 3.5 Design Science Research Cycles (Hevner, 2007)

A design science canvas is another method used to display the problem, define the requirements, knowledge base, research methods and strategies about the artefact that are used for the project. A design science canvas can be used as a sketch, monitoring tool or a summary for the project (Johannesson & Perjons, 2014). Figure 3.6 shows the design science canvas by Johannesson and Perjons (2014) and it's application.

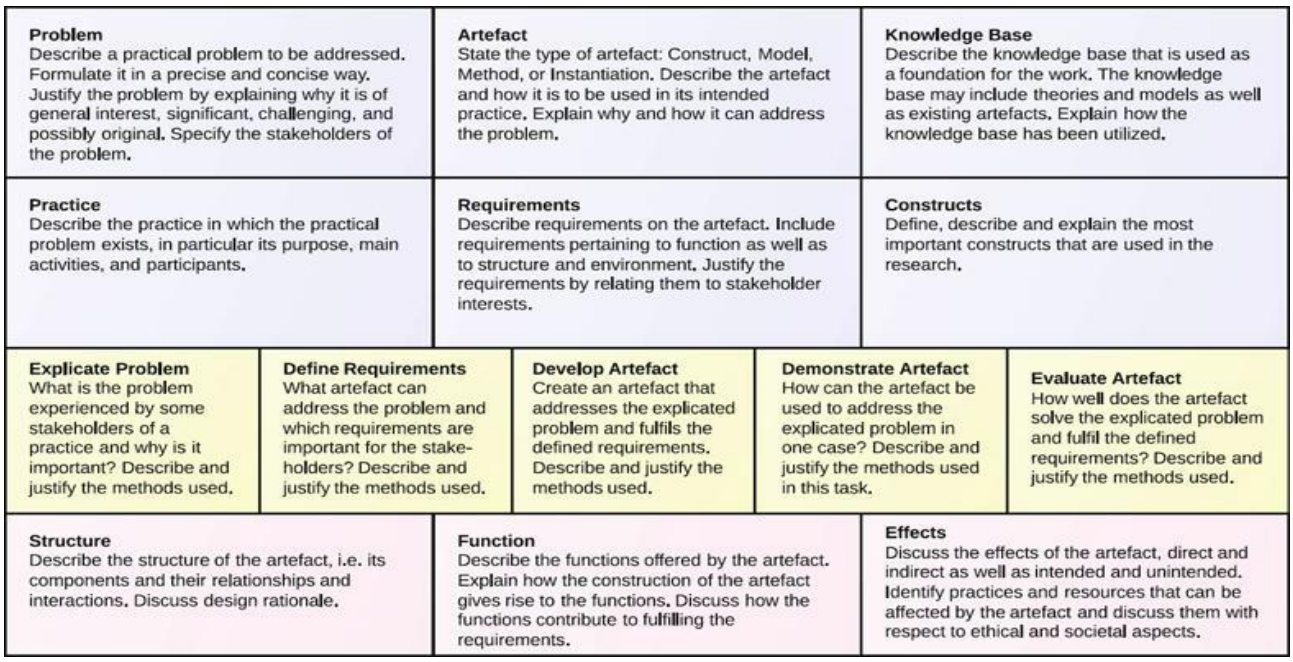


Figure 3.6 DSR Canvas (Johannesson & Perjons, 2014)

All three research methodologies described in this sub-section can be used to demonstrate the creation and analysis of an artefact. The Design Science Research Cycle by Hevner (2007) was selected for this study to demonstrate the artefact designed for this study – National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation in Namibia. Design science research cycles have a clearer presentation of the artefact design processes. The design science research cycles application to this study is displayed in figure 3.7.

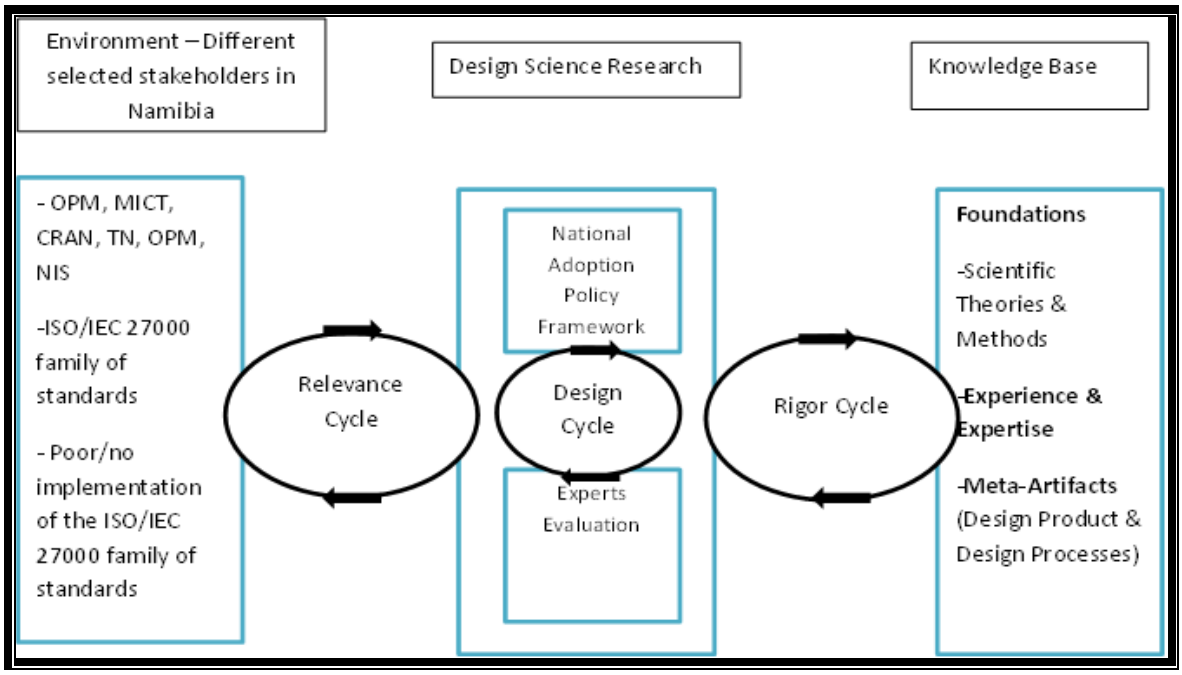


Figure 3.7 Design Science Research cycles application to the study

3.3.2 Design Science Research Process models

According to Peffers, Tuunanen, Rothenberger, and Chatterjee (2008), design science research process models consist of the following 6 process design attributes: Problem identification and motivation, define the objectives for a solution, design and development, demonstration, evaluation and communication. The six process design attributes were linked to the design science research cycles by Hevner (2007) and applied to this study as in section 3.2.1:

- ✓ Relevance Cycle
  - ➢ Problem identification and motivation
  - ➢ Define the objectives for a solution
- ✓ Design Cycle
  - ➢ Design and development
  - ➢ Demonstration
  - ➢ Evaluation
- ✓ Rigor Cycle
  - ➢ Communication

Several process models exist from authors such as Archer – 1984, Takeda, Veerkamp, Tomiyama, and Yoshikawam – 1990, Nunamaker, Chen, and Purdin – 1991 and Hevner, March, and Park – 2004 etc (Peffers et al, 2008). Worth mentioning for this study are the process models from Vaishnavi et al. (2017) and Peffers et al., 2008 as discussed below:

The model by Vaishnavi et al. (2017) shown in figure 3.8 starts with the awareness of the problem from new developments in the industry or knowledge base; the next step is the solution suggestion to the problem, then development and evaluation of the artefact are iteratively performed till a satisfactory artefact is developed and finally the conclusion.

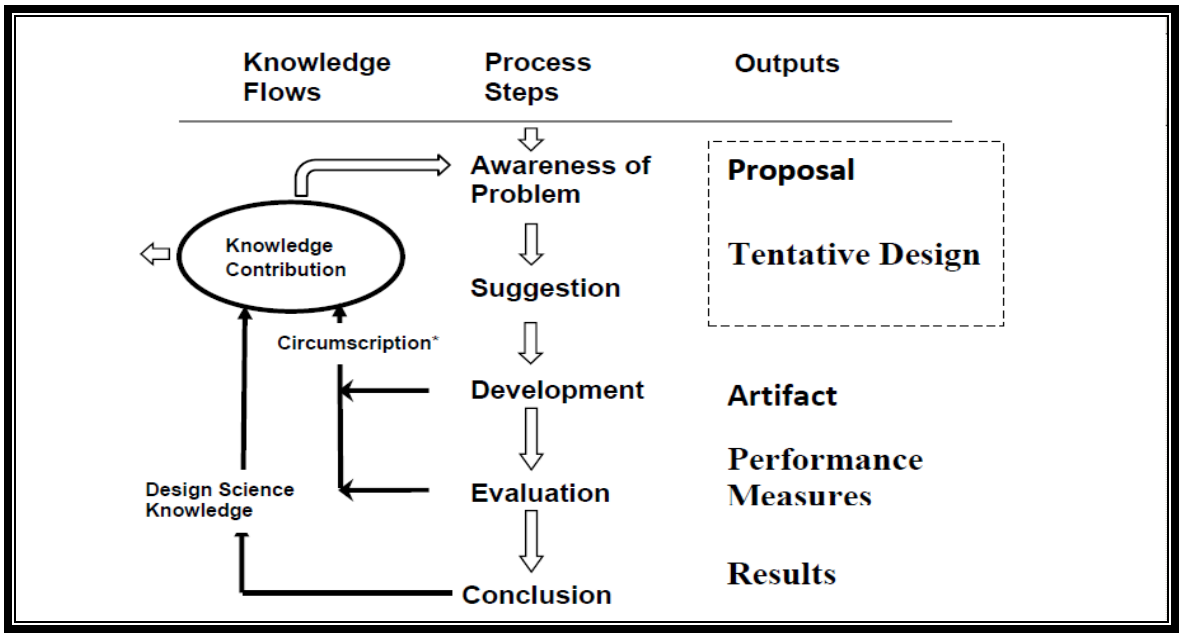


Figure 3.8 DSR process model (Vaishnavi et al., 2017)

The process model below (in figure 3.9) by Peffers et al. (2008) starts with either one of the following research entry points: problem centered initiation, objectives centered solution, design and development centered initiation and the client /context initiated. The model has six steps namely: the problem identification and motivation, define the objectives for a solution, design and development, demonstration, evaluation and communication.

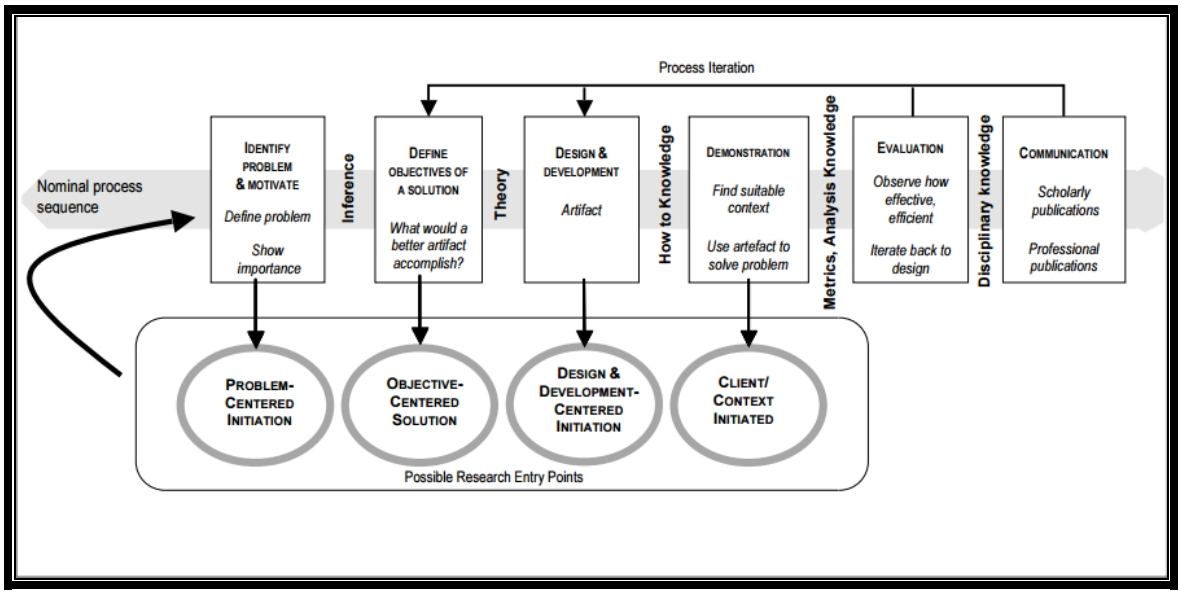


Figure 3.9 DSR process model (Peffers et al, 2008)

Table 3.6 compares the two process models discussed for this study. As depicted in table 3.1, the process model by Peffers et al. (2008) has an extra process design attribute namely demonstration which is missing in the process model by Vaishnavi et al. (2017). The communication process design attributes are used to demonstrate the artefacts functionality. Peffers et al. (2008)'s model also has more model entry points which give the researcher the flexibility of starting the research at any point and allowing them to do different types of research. This research took an inductive research approach and problem centered initiation. The model by Peffers et al. (2008) was appropriate for this study and it is discussed in section 3.2.3.

Table 3.6 Process models comparison

Design science research cycles and models entry points / Authors	Vaishnavi et al. (2017)	Peffers et al. (2008)
Relevance Cycle	Awareness of the problem	Problem identification and motivation
	Solution suggestion	Define the objectives for a solution
Design Cycle	Development	Design and development
	-	Demonstration
	Evaluation	Evaluation
Rigor Cycle	Conclusion	Communication
Entry Points	Development in the industry or knowledge base	Problem centered initiation Objectives centered solution Design and development centered initiation Client /context initiated.

3.3.3 Design Science Research Strategy Application to this Research

The DSR process model by Peffers et al. (2008) which follows the problem identification and motivation, defining the objectives for a solution, design and development of the artefacts, artefacts demonstration, artefact evaluation and artefacts communication was used for this project. The project is based on the problem centered approach. Figure 3.10 displays the process model by Peffers et al. (2008) and the sub-sections below describe the process model design attributes in detail.

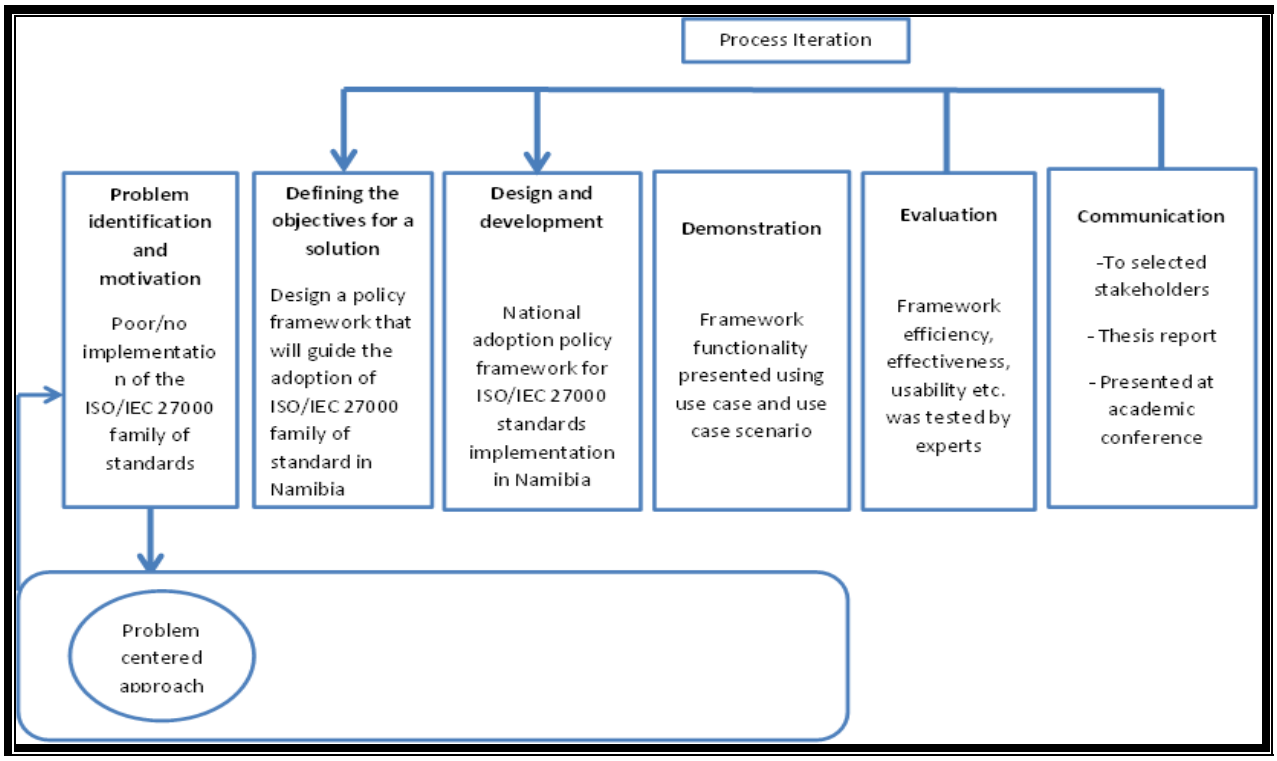


Figure 3.10 Process Model Application

Step 1 - Problem identification and motivation

Preliminary interviews were conducted with the OPM, MICT, CRAN, TN and NIS to determine the ISO/IEC 27000 family of standards implementation extent and to determine the factors affecting the implementation of the standards in Namibian organisations.

A gap analysis scale under section 2.7.1 was used to determine the ISO/IEC 27000 family of standards implementation extent. From literatures and preliminary interviews, it was established that the standard is at the 0 – requirement not implemented nor planned level.

ISO/IEC 27000 family of standards is used for information governance and to ensure that information security best practices are implemented in organisations. For the ISO/IEC 27000 family of standards benefits to be realized in Namibian organisations, the standard should be implemented.

A pilot study for a framework evaluation tool was conducted with master's students and experts from the industries. Few changes were recommended and amendments were made on the evaluation tool before deployment.

Step 2 - Define the objectives for a solution

The objectives of the study were to investigate: the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia, the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia, and lastly to design/constitute a policy framework that can guide the adoption of ISO/IEC 27000 family of standards into security best practices in Namibia.

Step 3 - Design and development

Based on critical literature reviews and preliminary interviews, a theoretical framework was designed and presented in Chapter 4. The framework served as a basis for the design of a policy framework that can guide the adoption of ISO/IEC 27000 family of standards to enable the implementation of security best practices in Namibia (see chapter 5).

Step 4 – Demonstration

The ISO/IEC 27001 policy framework functionality is presented using use case and use case scenario, and it is discussed in Chapter 5. Sehlhors (2007) describe use case as a representation of the process actions using multiple paths to achieve or abandon a goal and a single path through the use case as a use case scenario. The use case and use case scenario depict a high level process when implementing the ISO/IEC 27001 standard for an organisation.

Step 5 - Evaluation

An evaluation of the framework was done with experts from the different selected stakeholders. The purpose of the evaluation was to test whether the framework is efficient, operational, well designed and developed, and adaptable and customisable to provide the information security best practices. Different evaluation methods exist for this and a selected number is compared in table 3.7.

Table 3.7 Framework evaluation methods (Adapted from Hevner, March, Park & Ram, 2004)

Evaluation Methods	Description	Motivation for or against the method
Observational	**Case Study** – Detailed study of the artifact in business environment	Method not applicable as the artifacts will not be implemented and evaluated at the case site
	Field Study – Monitor use of artifact in multiple projects	This method is not applicable to this study, not a final product
Analytical	**Static analysis** – Examine structure of artifacts for static qualities (e.g. Complexity)	This was not used to test the artefact. We are not focusing on the structure of the framework but on the applicability
	Architecture Analysis – study how the artifact fit into technical information system architecture	This method is not appropriate for theoretical artifacts
	Optimisation - Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behaviour	The theoretical framework optimal properties are not tested. Artifacts will not be implemented and evaluated at the case site as there is no commitment from the stakeholders to do so
	Dynamic Analysis – Study artifact in use for dynamic qualities (e.g.	Artifact performance is not tested in this study so the method is not applicable

Evaluation Methods	Description	Motivation for or against the method
	performance)	
Experimental	**Controlled experiment** – study the artifact in controlled environment for qualities (e.g., usability)	Artifact usability is not tested, method not applicable
	Simulation models – execute the artifact with artificial data	Artifact performance is not tested in this study so the method is not applicable
Testing	**Functional (black box)** – testing helps to discover failures and defects.	Artifact functionality not tested, method not applicable
	Structural (white box) – Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation	Artifact is not implemented, method not applicable
Descriptive	**Informed argument** – uses information from knowledge base to build a convincing argument for artifact's utility	Information from the theoretical framework evaluation tool and literature will be used to design the national adoption policy framework for ISO/IEC 27000
	Scenarios – construction method constructs detailed scenarios around artifact to demonstrate its utility	This was used to demonstrate the artefact functionality

Descriptive evaluation using informed argument and case scenarios was used for this study. An informed argument was through literature reviews and data collected from the selected stakeholders. A use case scenario was used to demonstrate ISO/IEC 27001 policy framework functionality and it is discussed in Chapter 5.

Step 6 - Communication

The framework was distributed to the selected stakeholders for evaluation and secondly it was published as part of the thesis report. The framework was also published and presented at academic conferences (see Appendix C).

A case study was used as input to the above explained process model attributes to design the national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia. The case study research process is explained in section 3.2.2.1.

3.4 Research Quality

The quality of a qualitative research is measured with these criterion: credibility, transferability, dependability, conformability and trustworthiness (Maree, 2007; Oates, 2012; Pandey & Patnaik, 2014). The following sections discuss each criterion.

3.4.1 Credibility

Deals with ensuring that the research is carried out in the way it was intended to ensure an accurate presentation of the context (Maree, 2007; Oates, 2012; Pandey & Patnaik, 2014). This is achieved by applying triangulation to the data collection and data analysis methods (Maree, 2007; Oates, 2012; Pandey & Patnaik, 2014). Oates (2012) describes triangulation as a way of verifying findings and ensuring data validity by using more than one data collection methods.

Different triangulation methods exist for a research project (Oates, 2012):

- ✓ **Method triangulation** - Two or more data collection methods are used for the study
- ✓ **Strategy triangulation** - Two or more research strategies are used for the study
- ✓ **Time triangulation** - Research carried out at two or more different point times
- ✓ **Space triangulation** - Research carried out at two or more different countries

- ✓ **Investigator triangulation** - Two or more researchers carry out a study and then compare their findings
- ✓ **Theoretical triangulation** - Research study draws on two or more theoretical perspectives

Method triangulation was carried out in this study to ensure research credibility. Literature reviews, semi-structured interviews and questionnaires with stakeholders were the data collection methods used for this study. A literature review was conducted to help us understand the phenomenon. Semi-structured interviews were carried out to determine the implementation extent of the ISO/IEC 27000 family of standards and to identify factors affecting the implementation of the ISO/IEC 27000 family of standards in Namibia. To evaluate how efficient, operational, well designed, developed, adaptable and customisable a theoretical framework is, a questionnaire was sent out to experts.

3.4.2 Transferability

Deals with demonstrating whether the findings of one case can be generalised to another case (Oates, 2012; Pandey & Patnaik, 2014). To demonstrate transferability to others a detailed description is required from the researcher (Oates, 2012; Pandey & Patnaik, 2014). Transferability for this research was demonstrated using detailed descriptions of the problem statement, data collection and analysis tools and methods which were used for the design of a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia (see chapters 1 and 3).

3.4.3 Dependability

This is about determining whether the research findings, interpretations and conclusions speak to the data collected (Pandey & Patnaik, 2014). Dependability is determined by carrying out an audit of the research processes (Oates, 2012; Pandey & Patnaik, 2014). Data for this study were collected using literature reviews, semi-structured interviews and questionnaires with stakeholders. A pilot test of the questionnaire was conducted; few improvements were suggested and amendments were done. A self-administered online questionnaire was sent out to experts to evaluate the theoretical framework. A detailed description of the research process is in chapter 4 and 5.

3.4.4 Confirmability

This is about determining if enough information about the study has been given to verify if the findings can be linked to the research process (Oates, 2012; Pandey & Patnaik, 2014). Confirmability can be examined by carrying out a research audit through looking at the raw data, the summaries of the raw data and the data analysis (Oates, 2012; Pandey & Patnaik, 2014). Raw data collected for this study is presented in chapters 4 and 5. A detailed description of the methods and research process used for data collection and analysis is presented in chapters 3, 4 and 5.

3.4.5 Trustworthiness

This is about determining how much trust can be placed in the research study (Oates, 2012). To demonstrate trustworthiness, the literature review of the data collected for this study came from different sources, the study was evaluated at the conference proceeding and the theoretical framework was evaluated by experts.

3.5 Ethical Considerations

To ensure ethical conduct, an ethical consent was presented to the participants to voluntarily participate, and secondly anonymity and confidentiality of collected data were ensured.

3.5.1 Ethical Consent

To ensure that the ethical issues for this research project are well-known by the different selected stakeholders, a letter requesting permission to conduct research was prepared and distributed to the stakeholders (see Appendix A). The letter included the following statements and/or explanation as stated by Duke University (2013):

- ✓ The study is a research
- ✓ The purpose of the study
- ✓ Procedures used by the researcher to collect data from participants

- ✓ A description of the ISO/IEC 27000 family of standards benefits to Namibia that the framework can bring
- ✓ A statement describing that participants' confidentiality will be maintained
- ✓ An explanation that participation is voluntary and that the participant may discontinue at any time
- ✓ Whom to contact with questions about the study

The participants made an informed decision and they were free to withdraw anytime during the research. The data collected was not manipulated in any way to satisfy the required results.

3.5.2 Anonymity and Confidentiality

The evaluation tool did not collect personal information from respondents therefore they were not exposed in any way. The data were used for the purpose of research only and they were not distributed elsewhere.

3.6 Summary

Chapter three discussed the different methods, tools and strategies used for this study. A qualitative case study using an inductive research approach was used for this study as discussed. Time horizons, data collection and data analysis methods relative to the study were also discussed. Design science research methodology used to design the framework was also presented. Finally, ethical considerations were also discussed in this chapter.

The next chapter discusses data collected for this study to meet the research objectives and answer the research questions. The results from the collected data are discussed in the next chapter.

Chapter 4 – Data Collection and Results

4.1 Introduction

The previous chapter discussed the different methodologies used for this study. This chapter discusses the different data collected in this study and the results from analysing the collected data that answer the research questions and meet the study objectives. Data for this study were collected using literature reviews, interviews with selected stakeholders, pilot study and a questionnaire that was used to evaluate the framework. The data collection methods are discussed in the sections below. This chapter aims to answer the first two research questions for this study:

What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?

What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?

4.2 Literature Review

The literature review that was guided by the research questions was conducted using materials from the conference proceeding, journals, standard publications and textbooks. The literature review aimed to find methods used to determine the implementation extent of the ISO/IEC 27000 family of standards in organisations. The methods by Sell (2015) were determined to be applicable:

- ✓ Step 1: Select an industry standard security framework
- ✓ Step 2: Evaluate people and processes
- ✓ Step 3: Data gathering
- ✓ Step 3: Analysis

An industry standard security framework selected for this study is the ISO/IEC 27000 family of standard. ISO/IEC 27000 family of standards is categorised as a process (see figure 2.3 in section 2.2.3), and experts from selected organisations assisted with the evaluation of the processes implemented in their organisations. Data gathering and analysis were conducted quantitatively for this study as shown in this chapter and section 5.6 respectively.

The factors affecting the adoption of the ISO/IEC 27000 family of standards were identified from the literature review as well and they are shown below:
Identifying the organization's assets; weak team experience, deployment of the wrong personnel; resistance to change; unclear understanding of standards; lack of top management involvement; culture; lack of discipline; improper documentation; inadequate budget; poor enforcement of policies and procedures (AbuSaad et al., 2011; Kiilu & Nzuki, 2015).

The identified factors affecting the adoption of the ISO/IEC 27000 family of standards might affect organisations in Namibia when adopting the standards. Management and information security experts involved in the standard adoption process should do a thorough review of the identified factors for a successful implementation of the standard.

4.3 Interview

Based on literature review findings in section 4.2, a semi-structured interview questionnaire in Appendix B was developed to investigate the baseline implementation of ISO/IEC 27000 family of standards in Namibian organisations. A preliminary interview was conducted with the OPM, MICT, CRAN, TN and NIS as these organisations offer rich information about the topic being studied. The interview also aimed to investigate the factors affecting the implementation of the ISO/IEC 27000 family of standards in Namibia.

The collected data were organized and prepared for analysis as presented in table 4.1.

Table 4.1 Collected data from semi-structured interviews

Semi-Structured interview questions	OPM	MICT	CRAN	NSI	TN
1. Is the ISO 27000 family of standards implemented in your organisation?	No	No	No	No	No
2. Does your organisation have documented Information Technology security standard policies?	Yes, we have policies but we don't follow security standards	Yes, we have policies but they are not structured according to ISO	Yes	Yes	Yes, we have policies and we are busy updating them
3. What are the factors affecting the adoption of ISO 27000 family of standards?	We don't have people certified in ISO standard and we will select qualified employees to certify	Employees are not trained and are not certified in ISO 27001	Employees are aware of the standard but they need training	Employees are not trained	Information security experts need to be trained on security standards
4. Who governs security policies?	OPM	OPM	MICT	OPM and other stakeholders	NIS
5. Do you have any plans of implementing the ISO 27000 family of standards as a security solution to the current challenges?	Yes, The Cyber security bill is before parliament and ISO 27000 family of standards is part of this bill	Yes, Cyber security bill is before parliament	Yes, Cyber security bill is before parliament currently	Yes, When the cyber security bill is approved	Yes

To analyse the data collected from the preliminary interviews with selected stakeholders, the steps from Creswell (2003) were used as presented in section 3.2.2.1:

The researcher read through all the data collected to interpret the data and to come up with results. The collected data in table 4.1 were organised (coded) according to the interview questions (column 1) and the organisation interviewed (row 1). The questions were further used to generate themes/categories to describe the data. The themes generated were:

- ✓ Security landscape => question 1 and 4
- ✓ Factors affecting the adoption/implementation of ISO 27000 => question 2 and 3
- ✓ Mitigating strategy => question 5
- ✓ Benefit of implementing ISO 27000 Standards => Was informed by the literature review

The data from the different categories/themes were summarised and they are depicted in table 4.2 and they are supported by the literature review. Each column headings are the different categories and each column consist of the questions and answers for the specific category.

Table 4.2 Summary of semi-structured interview response and, the benefit and mitigating strategy of ISO/IEC 27000

Security landscape	Factors affecting the adoption/implementation of ISO 27000	Mitigating strategy	Benefit of implementing ISO 27000 Standards
To gauge the security landscape. The question "Is the ISO 27000 family of standards implemented in your organisation?" was used and responses showed: No the standard is not implemented. In response to "Who governs security policies?", the stakeholders stated that NIS, MICT and OPM are responsible for security policy governance	In response to "What are the factors affecting the adoption of ISO 27000 family of standards?" Weak team experience or deployment of the wrong personnel was noted, the respondents said that "employees are not trained and are not certified in ISO 27001". In response to question two "Does your organisation have documented Information Technology security standard policies?" the respondents noted that they have documented polices but not according to ISO/IEC 27000 - poor enforcement of policies and procedures	When asked do you have any plans to implement the ISO 27000 family of standards as a security solution to the current challenges? The stakeholders stated "Yes, the Cyber security bill is before parliament and ISO 27000 family of standards is part of this bill".	Cost benefits of ISO27000 implementation were identified as: 1. Protects crucial resources 2. Manages risks more efficiently 3. Improves and maintains customer confidence 4. Shows that they are adapting to international best practice 5. Avoids brand damage and changes its information security posture alongside technological developments

Data interpretation:

For gap analysis the levels by Kosutic (n.d.-b) below were selected to indicate the ISO/IEC 27000 family of standards implementation extent in Namibia:

- ✓ 0 – requirement not implemented nor planned
- ✓ 1 – requirement is planned but not implemented
- ✓ 2 – requirement is implemented only partially so that full effects cannot be expected
- ✓ 3 – requirement is implemented, but measurements, reviews and improvements are not performed

- ✓ 4 – requirement is implemented and measurements, reviewss and improvement are performed regularly

The semi-structured interview findings in table 4.2 depict that the standard is not implemented and that organisations in Namibia will consider the standard after the Cyber Security Bill is discussed and approved in parliament. According to Aipinge in an article written by Olivier (2017), the Cyber Security bill which is still in a draft mode was withdrawn from parliament for further consultation with the public. The standard is not implemented and the draft Cyber Security bill does not mention anything on information technology governance standards (Minister of Information Communications and Technology, n.d.), therefore Namibia falls under the level 0 – standards not implemented nor planned.

The gap analysis application and all findings in table 4.2 and section 4.2 informed the design of a theoretical framework as presented in section 5.4.

4.4 Summary

This chapter discussed the data collection and results on the factors that affect the implementation of the ISO/IEC 27000 family of standards from literatures and the ISO/IEC 27000 family of standards implementation extent in Namibian organisations from preliminary interviews with selected stakeholders.

The next chapter will discuss the framework design process.

Chapter 5 – Framework Design Process

5.1 Introduction

The previous chapter discussed the findings of literature reviews on what affects the adoption of the ISO/IEC 27000 family of standards and the preliminary interview data collected to determine the implementation extent of the ISO/IEC 27000 family of standards in Namibian organisations. The findings will inform the design of the policy framework for ISO/IEC 27000 family of standards adoption.

This chapter discusses the design and evaluation of the theoretical framework, how a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia was constituted to mitigate information security risks. The 6-phase design science research process model by Peffers et al. (2008) was used for the framework design process. The steps are: problem identification and motivation; define the objectives for a solution; design and development; demonstration; evaluation and communication, and they are discussed in sections 5.2 through 5.7. This chapter aims to answer the main research question:

How can a policy framework be constituted to guide the adoption of ISO/IEC 27000 family of standards into security practice?

5.2 Problem Identification and Motivation

A preliminary interview was conducted with the OPM, MICT, CRAN, TN and NIS, and with the gap analysis scale discussed in sections 2.7.1 and 4.2, it was established that Namibia is at the 0 level – requirement not implemented nor planned stage. ISO/IEC 27000 family of standards help organisations to manage financial information, intellectual property, employee details or third party information (ISO, n.d.-a) and despite these benefits the standard is not implemented in Namibian organisations.

The study designed a national policy framework to guide the adoption of the ISO/IEC 27000 family of standards in Namibia into security best practices. The artefact will encourage the realisation of the standard's benefits and mitigate information security risks in Namibia organisations. The information security risk can be social engineering, unauthorized disclosure of information or passwords, access to the network by unauthorised persons, errors in maintenance, loss of electricity, human or natural disasters, malfunction of equipment, destruction of records, theft of hardware, fire, loss of productivity, financial loss, legal implications and organisational blackmail as presented in section 2.7.3.

5.3 Define the Objectives for a Solution

For Namibian organisations to gain the benefits of the ISO/IEC 27000 family of standards and help mitigate information security risks, the study aimed to:

- ✓ Investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia
- ✓ Investigate the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia
- ✓ Design/constitute a policy framework that will guide the adoption of ISO/IEC 27000 family of standard into security best practices in Namibia

5.4 Design and Development

This section discusses the theoretical framework design process and the framework implementation guidelines process.

5.4.1 Theoretical Framework

A theoretical framework was developed based on the literature review findings in chapter 2 and section 4.2, and data collected from preliminary interviews with stakeholders in section 4.3 using the following steps from Vinz (2017) as already mentioned in section 2.8:

- ✓ Select key concepts listed below
  - ➢ Problem
  - ➢ Objective
  - ➢ Research question
- ✓ Define and evaluate relevant concepts, theories, and models
- ✓ Consider adding other elements to your theoretical framework

The following subsections present the application of Vinz's steps to this study.

5.4.1.1 Select key concepts

This step involves the design of the theoretical framework using literatures and preliminary interviews, and the output of the process about the problem statement, the research problem, research objectives and questions as follows:

- ✓ **Problem statement** – The ISO/IEC 27000 family of standards provides a globally recognised information security management framework best-practice (ItGovernance, 2015). There is a 100% growth in internet usage in Namibia

- ✓ According to IT News Africa (2016), in November 2015 Namibia was the second most attacked country after being the most targeted by cybercriminals and this was revealed in December 2015. To what extent is Namibia implementing these best practices to ensure secure cyber experiences for her citizens?
- ✓ **Problem** – The problem under investigation was then framed as "How can a policy framework be constituted to guide the adoption of ISO/IEC 27000 family of standard into security practice?"
- ✓ **Objectives** – The objectives of the study were to investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia and investigate the factors affecting the adoption of ISO/IEC 27000 family of standards. A theoretical framework was designed to inform the stakeholders on the extent of the implementation of security best practices in Namibia and the factors affecting the adoption of the standards.
- ✓ **Research questions**:
  - ➢ What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?
  - ➢ What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?

5.4.1.2 Define and evaluate relevant concepts, theories, and models

Concepts, theories and models relevant to this study are discussed in chapter 2. The major concepts were identified as information security, information security governance, information security policy and theoretical framework. In order to implement the ISO/IEC 27000 family standards, the following theories were found to be pivotal: ISO/IEC 27000 family of standards, gap analysis, ISMS pillars, information security pillars and security controls. Existing models applicable for this research were ISO/IEC 27000 family of standards, NIST 800-53, COBIT and ITIL.

5.4.1.3 Consider adding other elements to your theoretical framework

The interviews and surveys with the regulatory board (CRAN), ISPs and government departments revealed that the standard is not implemented. Namibia is a member of ISO and to gain the benefits it should implement relevant ISO standards. The following factors typical to Namibia were identified and will be added to the framework:

- ✓ Namibia is at the 0 level – requirement not implemented nor planned level
- ✓ Weak team experience or deployment of the wrong personnel
- ✓ Employees are not trained and they are not certified in ISO 27001
- ✓ Poor enforcement of policies and procedures
- ✓ To mitigate information security risks in Namibia, it was said the Cyber Security Bill is before parliament and ISO 27000 family of standards is part of this bill.

Other factors that affect the adoption of the ISO/IEC 27000 family of standards are presented in section 4.2. The implementation and adoption of the ISO 27000 standard in Namibia might also be influenced by the factors mentioned.

From the literature (section 4.2) and survey (section 3), the key components to the assessment of the extent of adoption/implementation were identified as:

1. Security landscape
2. Factors affecting the adoption and implementation
3. Mitigating strategy
4. Cost benefit analysis
5. Gap analysis

These components informed the theoretical framework design. The relationships are shown in figure 5.1.

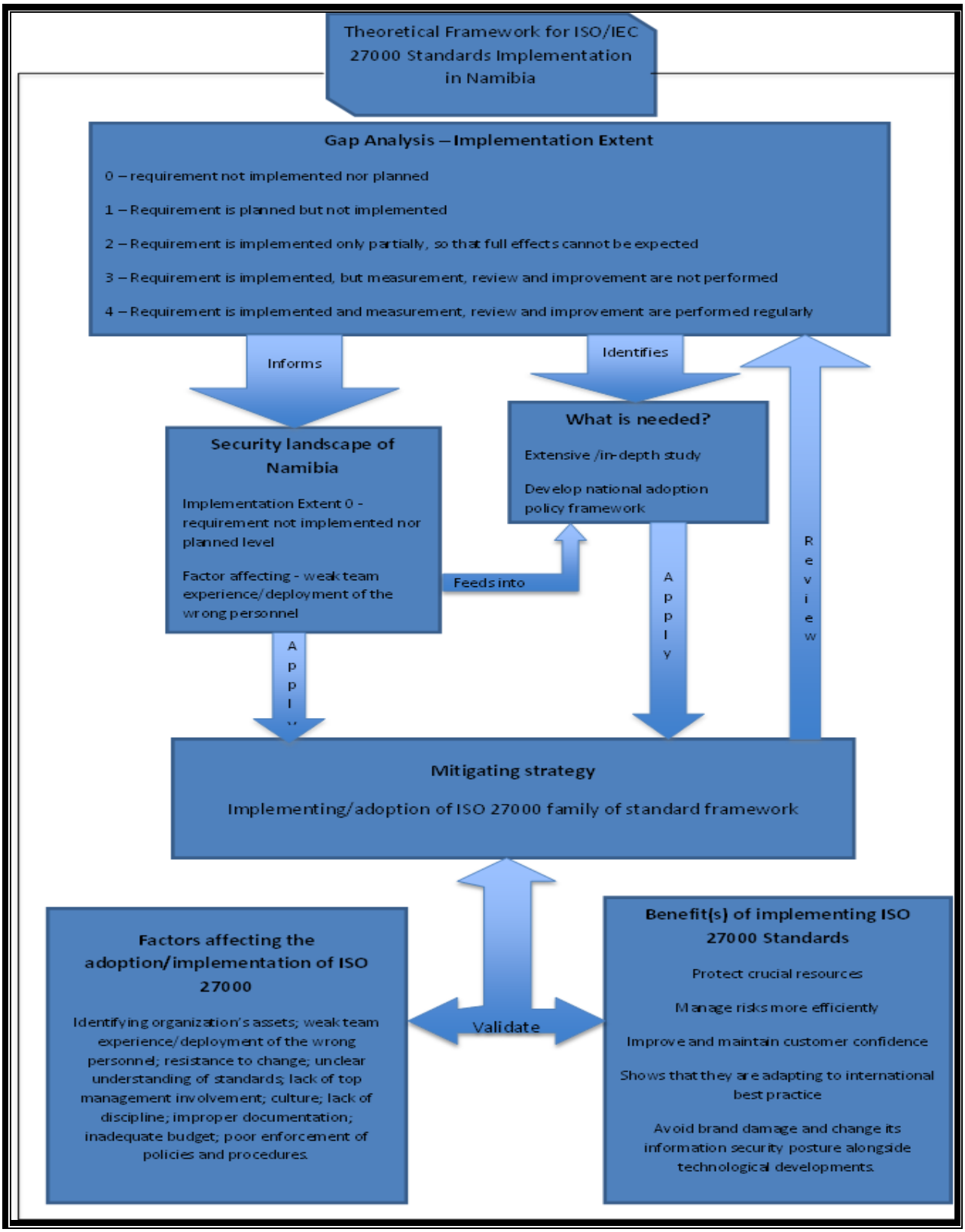


Figure 5.1 Theoretical Framework (Tjirare & Bhunu Shava, 2017)

The theoretical framework shows the security of Namibia, possible mitigating strategies, the benefit of implementing the ISO/IEC 27000 standard, gap analysis scale, factors affecting the implementation and what still needs to be done to improve the security. When there is a clear understanding of the security posture of an organisation, mitigation strategies can be evaluated and the best selected for adoption. However before adopting a strategy the benefits need to be well understood as these will inform the gap analysis and the establishment of factors that are critical to the success. Once this is clear, steps can be listed which need to be effected to improve the posture. The framework presented in figure 5.1 is entirely based on the case study findings and it is informed by the literature review.

5.4.2 Framework Implementation Guidelines

To guide the implementation of the framework for ISO/IEC 27000 standards implementation, figure 5.2 was designed as the framework implementation guidelines. The framework implementation guideline has three layers namely the information security (infosec) controls for ISO/IEC 27001 standard (outer layer), information security management system (ISMS) pillars (middle layer) and the information security pillars (inner layer).

For example, if an organisation was to implement the policies for information security control it would need the:

ISMS pillars - for efficient, comprehensive, and cost-effective information security policies (Olsen, 2014)

Information security pillars – for the protection of information against unauthorized person and unauthorized modification, ensuring availability of information, verification of an individual's identity and proving the originality of an action.

The three pillars are then classified as:

- ✓ Infosec controls for ISO/IEC 27001 standard (outer layer) – The assets to be implemented

- ✓ ISMS pillars (middle layer) – Assets Operators
- ✓ Information security pillars (inner layer) – Assets and operators protector

The application of the pillars to the study are discussed in the next 3 sections.

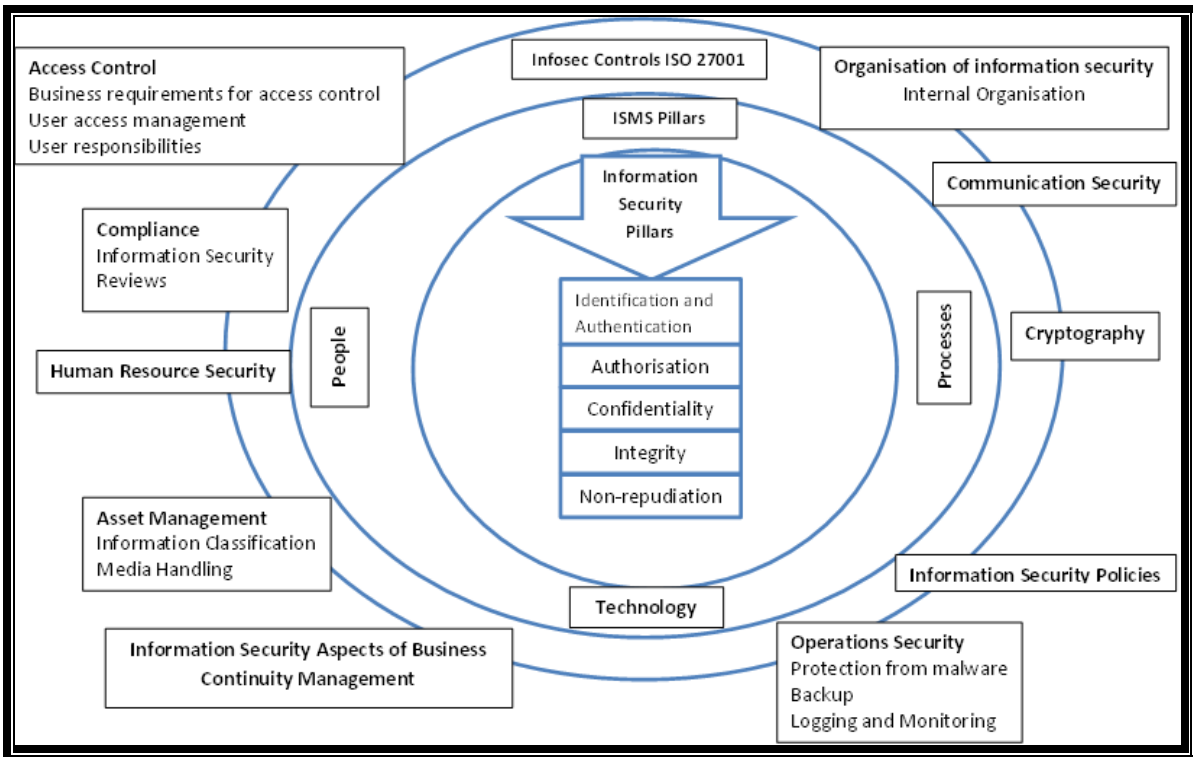


Figure 5.2 National adoption policy framework implementation guidelines

5.4.2.1 InfoSec Controls for ISO/IEC 27001 Family of Standard

ISO/IEC 27001 has 14 control domains and 11 control domains were used for this study. The control domains used deal directly with information security. The following controls were not tested for this study because they don't deal directly with information security: physical and environmental security; system acquisition; development and maintenance; and supplier relationships. However, they are recommended when Namibian organisations implement the national adoption policy framework depending on the organisational needs because they can assist to mitigate the information security risk.

The following controls were tested with the framework evaluation tool (Appendix D) that was sent out to experts: information security policy; compliance; information security aspects of business continuity management; communication security; operations security; cryptography; access control; asset management; human resource security; organisation of information security and information security incident management, and they are depicted in the outer layer of the national adoption policy framework implementation guidelines. Almost all participants agreed that the implementation of the security controls is important as discussed in section 5.6.2.1-2-A.

Info Sec controls for ISO/IEC 27001 family of standard can be implemented by all types and sizes of organisations to mitigate information security risks (Granneman, 2013). Namibian organisations can select Info Sec controls for ISO/IEC 27001 family of standards for implementation based on their needs (BSI, 2009).

5.4.2.2 ISMS Pillars

ISMS consist of three pillars namely people, processes and technology. The framework implementation guideline (figure 5.2) depicts the ISMS pillars in the middle layer. The three pillars are explained below as to how they can be used to successfully implement the national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia.

A. People

The people's pillar deals with two types of people, the users of the ISO/IEC 27001 framework processes (everyone in the organisation) and the information security experts (Dutton, 2017). In order to have a successful national adoption policy framework, users should be trained on all security controls being implemented by organisations in Namibia.

Information security experts need to have the right qualifications and be competent to implement the right ISO/IEC 27001 controls to mitigate information security risks. Information security experts and the management need to be knowledgeable on all components of the national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia.

B. Processes

The processes pillar consists of management systems, governance frameworks, best practices and IT audits as mentioned in figure 2.3 in section 2.2.3 (Dutton, 2017). The national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia falls under this pillar. The different components of the national adoption policy framework will guide the information security experts and the management on how to successfully implement the ISO/IEC 27000 family standards in Namibian organisations.

C. Technology

Different technologies implemented for the national adoption policy framework will need the people's pillar for operation and implementation, and the processes pillar as guidelines (Olsen, 2014; Dutton, 2017). Technologies prevent or reduce the risk of information technology (Dutton, 2017). Namibian organisations need to select the right technologies for the different ISO/IEC 27001 controls to gain the standard benefits.

5.4.2.3 Information Security Pillars

In order for the national adoption policy framework to be successfully implemented, the information security pillars need to be considered. The information security pillars are confidentiality, integrity, availability, non-repudiation and authentication and they will protect the Info Sec controls for ISO/IEC 27001 family of standards and the ISMS pillars against information security attacks (United States Naval Academy, n.d.; Arrunadayy, 2017).

5.5 Demonstration

Framework application is demonstrated using use case and use case scenario. The use case in figure 5.3 demonstrates the ISO/IEC 27001 implementation requirements for Namibian organisations. When implementing ISO/IEC 27001, a continuous PDCA cycle is used to manage the ISMS as explained in section 2.6.1.2.

The ISO/IEC 27001 implementation requirements are used with this PDCA cycle stage as discussed in section 2.6.1.2 (Fedco, 2015):

- ✓ PLAN – Context of the organisation, leadership, planning and support
- ✓ DO – Operations
- ✓ CHECK – Performance
- ✓ ACT - Improvement

When implementing the control objectives and controls in Annex A of the ISO/IEC 27001 standard, the control objectives and controls are part of all the standard requirements.

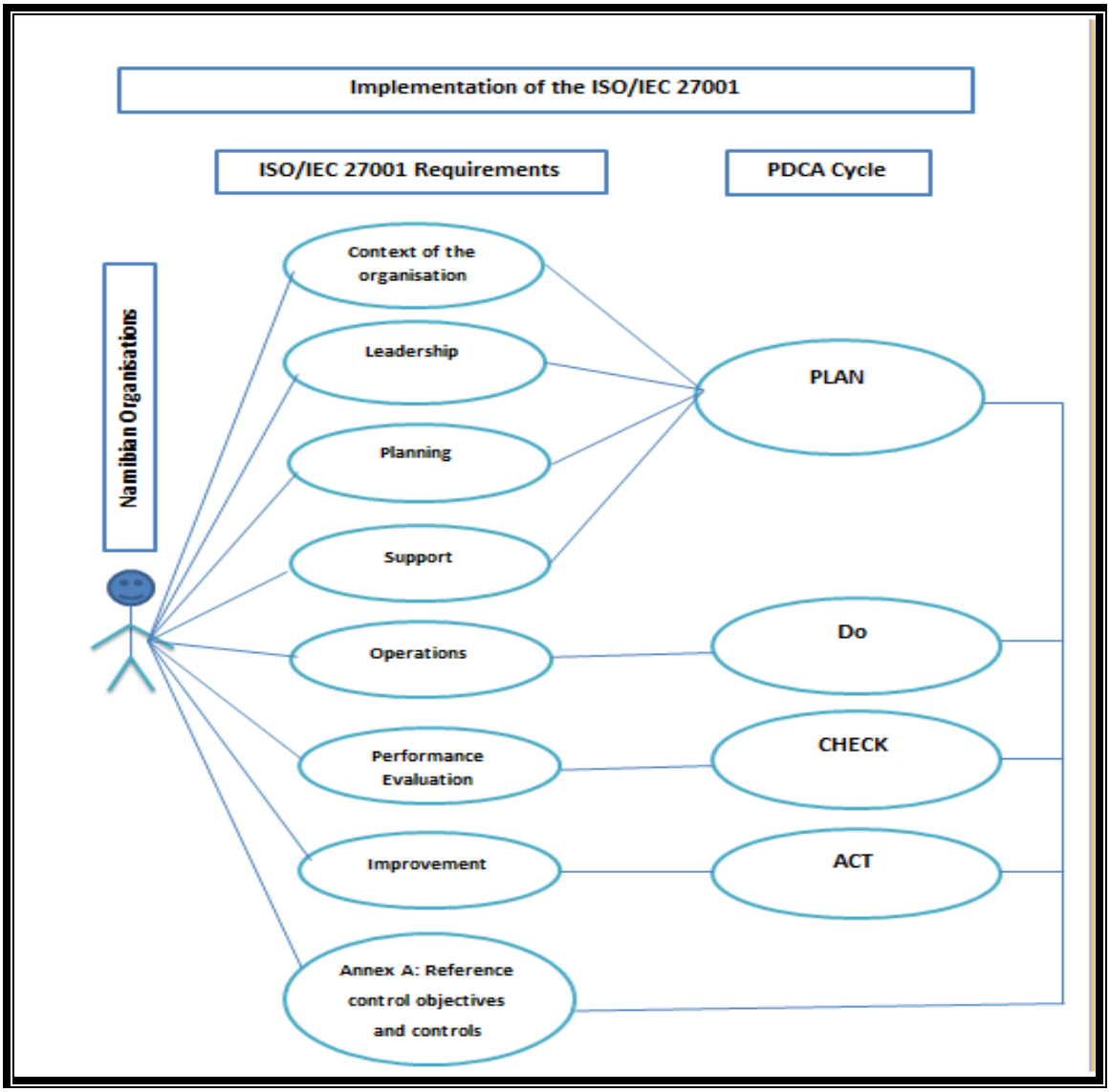


Figure 5.3 Implementation of the ISO/IEC 27001

Table 5.1 depicts use case scenarios of the ISO/IEC 27001 requirements that are prepared using the PLAN stage of the PDCA cycle. The table shows the ISO/IEC 27001 requirements in the first column and the implementation requirements to be used for the National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation in Namibia.

The implementation requirements column lists the requirements and an explanation of each requirement.

Table 5.1 Use case scenarios for PLAN (ISO/IEC, 2013b; Kosutic, n.d.-a)

ISO/IEC 27001 Requirements	**Implementation Requirements**	
0 Introduction	The framework aimed to guide the adoption of ISO/IEC 27000 family of standard into security best practice in Namibia	
1 Scope	Namibian organisations	
2 Normative References	ISO/IEC 27000 - ISMS overview and vocabulary ISO/IEC 27001 - ISMS requirements ISO/IEC 27002 - Code of practice for information security controls ISO/IEC 27003 - ISMS implementation guidance ISO/IEC 27004 - Information security management measurement	
3 Terms and Definitions	ISO/IEC 27000 - ISMS overview and vocabulary	
4 Context of the organisation	4.1 Understanding the organisation and its context	Understanding the organisation's internal and external context. **Internal context** => Organisational knowledge, organisational structure, company values, company culture, ICT infrastructure and available resources **External context** => Legal and regulatory requirements, social environment, competitive environment, cultural environment, economic environment and political environment
	4.2 Understanding the needs and expectations of interested parties	Organisation needs to determine: Interested parties relevant to ISMS => Employees, clients, partners, suppliers, local authorities

ISO/IEC 27001 Requirements	Implementation Requirements	
		Requirements of relevant parties
	4.3 Determining the scope of the information security management system	Organisation determines the boundaries and applicability of the ISMS to establish its scope. When determining this scope consider: The internal and external context under 4.1 The requirements under 4.2 Interface and dependencies between activities
	4.4 Information security management system	The organisation needs to establish, implement, maintain and continually improve an ISMS according to the requirements of this international standard
5 Leadership	5.1 Leadership and commitment	Top management shall demonstrate leadership and commitment to the ISMS by: ✓ Establishing information security policies and objectives ✓ Ensuring availability of resources necessary for the ISMS ✓ Communicating the importance of information security ✓ Making sure ISMS is integrated within the company process ✓ Promote continual improvement of the ISMS
	5.2 Policy	Top management shall establish an information security policy
	5.3 Organisational role, responsibilities and authorities	Ensuring fulfilment of ISO 27001 requirements Reporting on effectives of ISMS
6. Planning	6.1 Actions to address risks and opportunities	The action to address risks and opportunities are: ✓ General actions => Consider issues referred to in 4.1 and requirements referred to in 4.2 and determine the risk and opportunities to be addressed.

ISO/IEC 27001 Requirements	Implementation Requirements	
		✓ Information security risk assessment ✓ Information security risk treatment
	6.2 Information security objectives and planning to achieve them	Establish information security objectives and at relevant functions and levels
7. Support	7.1 Resources	Ensuring availability of resources
	7.2 Competence	Define necessary skills to perform the task Ensure employees have needed training and experience
	7.3 Awareness	All employees must be aware of the information security policy Employees should know the implication of not following the ISMS rules Employees should know what to do and why they should perform a task
	7.4 Communication	Define the need for internal and external communication Define what and when information should be communicated and by whom
	7.5 Documented Information	The organisation's ISMS should include: Information that provides guidance on how processes are conducted Information that is evidence of performed activities or achieved results Make sure that the appropriate format and media are used for documenting

When implementing the national adoption policy framework for ISO/IEC 27000 standards, it is recommended to look at the first five standards of the ISO/IEC 27000 as they will provide guidance at the different PDCA cycles. The standards are discussed under section 2.6.1.1 – 2.6.1.5

5.6 Evaluation

The framework evaluation was performed using the descriptive evaluation using informed argument and use case scenarios as explained in section 3.3.3 – Step 5 (Hevner, March, Park & Ram, 2004). The framework was evaluated using argumentation from literature reviews, preliminary interviews and academic publications, and these are presented in chapters 2 and 4, and Appendix C.

Use case scenarios were designed to demonstrate the framework implementation process. These are presented in section 5.5.

The next sections discuss the theoretical framework evaluation process which began with the design of an expert evaluation tool, and the tool was piloted and finally deployed.

5.6.1 Framework Evaluation Tool Design

A questionnaire with mostly closed ended questions for the theoretical framework components evaluation and open ended questions for further explanation or respondent's opinion was designed as the theoretical framework evaluation tool.

5.6.2 Framework Evaluation Tool Pilot Study

A pilot survey was conducted with Information Security Master's students at the Namibia University of Science and Technology and several experts from the industry. The purpose of the pilot study was to verify the functionality and usability of the evaluation tool. Few amendments were specified during the pilot survey and changes were made before the evaluation tool was sent out to selected stakeholders for the evaluation tool recommended changes. Figure 5.4, 5.5 and 5.6 list the different amendments suggestion on the evaluation tool.

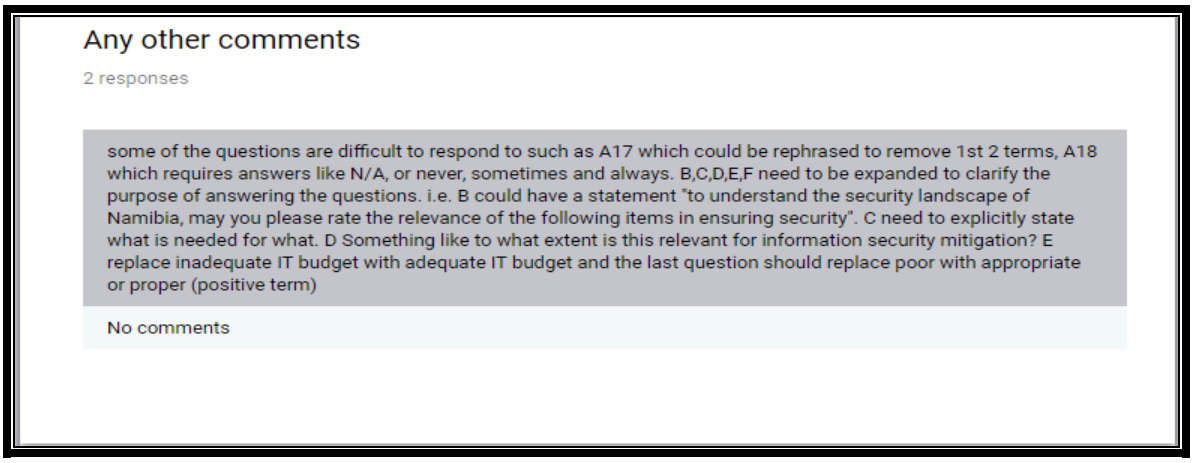


Figure 5.4 Pilot Survey Data 1

Figure 5.5 Pilot Survey Data 2

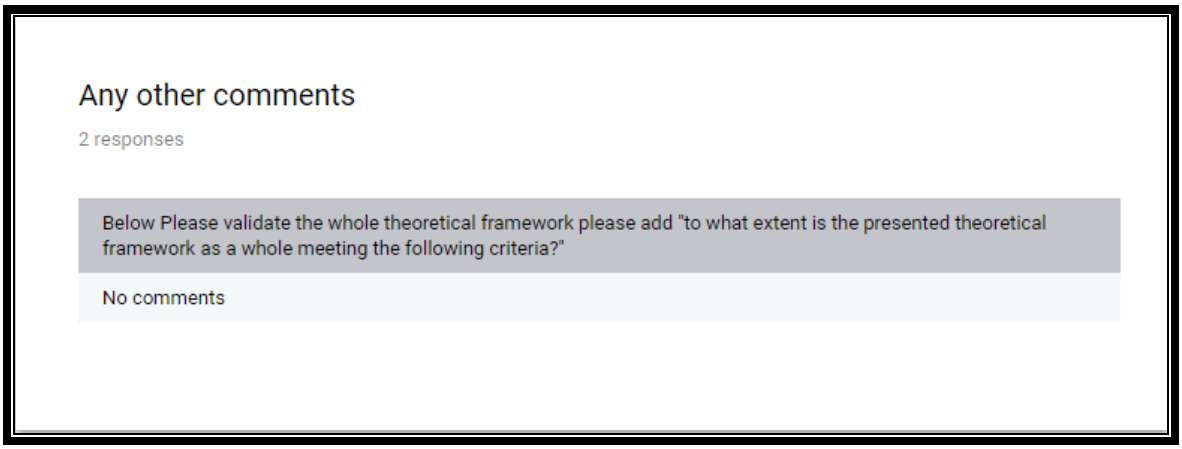


Figure 5.6 Pilot Survey Data 3

5.6.3 Framework Evaluation

The theoretical framework evaluation tool had six sections (see Appendix D for the theoretical framework evaluation tool). Section one described the purpose and requirements of the evaluation tool. Section two described and presented the theoretical framework. Section three was about the participants' biographical information. Section four evaluated the importance and relevance of the following:

- ✓ Gap analysis implementation extent
- ✓ Security landscape of Namibia
- ✓ What is needed to mitigate information security risks in organisations
- ✓ Implementation or adoption of ISO 27000 family of standard framework as information security risk mitigation strategy
- ✓ Factors affecting the adoption of ISO/IEC 27000 standards
- ✓ The benefits of implementing ISO 27000 family of standards

Section five evaluated the importance and relevance of the information security controls. Section six evaluated the whole theoretical framework. Section four and five evaluated the importance and relevance of the same criteria to validate the participants' responses.

The evaluation tool used a four-point Likert scale choice to measure the different options under each section. The options were from very important to least important, very relevant to least relevant and strongly agree to strongly disagree. The purpose of the evaluation tool was to find out the relevance of the framework and the ISO/IEC 27000 security controls from selected stakeholders.

5.6.4 Framework Evaluation Results

5.6.4.1 Biographical Information

The purpose of this section was to collect biographical information of different stakeholders. The following information was collected from the stakeholders: gender, age, position, information security years of experiences and organisation.

Sixty four percent of the participants were male, and thirty six percent were female as presented in Table 4.3. Table 4.4 shows the participants' age group, and 45.5% of the participants are in the age group 20 - 30 and 31 -40, and 9.1 % are in the age group 41 -50 and there was no representation of the age group 51 - 60. Participants' position, information security years of experiences and organisation are presented in Tables 5.2 – 5.6.

Table 5.2 Stakeholders' Gender

Gender	Total	Percentage
Male	7	64
Female	4	36
Total respondents:	11	100

Table 5.3 Stakeholders' age group

Age group	Total	Percentage
20 - 30	5	45.5
31 - 40	5	45.5
41 - 50	1	9.1
51 - 60	0	0
Total respondents:	11	100

Table 5.4 Stakeholders' Position

Position	Total
Head of Information Technology	1
IT Technician	2
System Administrator	0
Information Security Expert	2
Standard officer	1
Information Security Risk Assessor	1
Application Specialist	1
ICT trainer	1
IT Manager	1
Snr Engineering Technician	1
Total respondents:	11

Table 5.5 Stakeholders' years of experiences in information technology

Information Security Years of Experiences	Total
0 - 5	6
6 -10	2
11 - 20+	3
Total respondents:	11

Table 5.6 Stakeholders Organisation

Organisation	Total
Office of the Prime Minister	1
Ministry of Information and Communication Technology	1
Communication Regulatory Authority of Namibia	1
Namibia Institute of Standards	1
Telecom Namibia	4
Namibia Institute of Pathology	1
Academia	1
Higher education	1
Total respondents:	11

5.6.4.2 Theoretical Framework Evaluation

This section measured the importance and relevance of the different theoretical framework categories to find out the views of selected experts on the theoretical framework. The following categories were measured and are discussed below: the gap analysis implementation extent, security landscape of Namibia, what is needed to mitigate information security risks in organisations, implementation or adoption of ISO/IEC 27000 family of standards framework as an information security risk mitigation strategy, factors affecting the adoption of ISO/IEC 27000 standards and the benefits of implementing the ISO/IEC 27000 family of standards.

A four-point Likert scale set of choices were used to measure the different options under each section. The options were from very important to least important, very relevant to least relevant and strongly agree to strongly disagree. All sub-sections under the theoretical framework evaluation section tested the relevance and importance of the same categories. The definitions of the two synonyms according to the Collins dictionary:

Relevant - Something that is relevant to a situation or person is important or significant in that situation or to that person (Collins, 2018b).
Important - Something that is important is very significant, is highly valued, or is necessary (Collins, 2018a).

The purpose was to validate the respondents' answers against the choices (important and relevant). The same question was asked in different ways and the responses were supposed to match (speak to the same thing as synonyms were used for the same questions) in each category; however, the answers were contradicting. For example, the respondent cannot choose that a security control is very relevant and then at the next category the same security control is not important.
The results showed that either the participants didn't understand the question or they were not reading the question. The matching options below were used throughout this section; the ones highlighted green are the matching results and the ones highlighted red are contradicting results. The Microsoft excel document IEC 27000 Standards Implementation in Namibia Response Validation.xlsx shows respondents validation. To represent the outliers each category has a matching and contradicting subcategory.

Matching Results

Very Relevant	Relevant	Not Relevant	Least Relevant
Very Important	Important	Not Important	Least Important

Very Relevant	Relevant	Not Relevant	Least Relevant
Important	Very Important	Least Important	Not Important

Relevant	Very Relevant	Least Relevant	Not Relevant
Very Important	Important	Not Important	Least Important

Contradicting Results

Very Relevant	Relevant	Not Relevant	Least Relevant
Not Important	Least Important	Very Important	Important

Least Relevant	Not Relevant	Relevant	Very Relevant
Very Important	Important	Not Important	Least Important

Very Relevant	Relevant	Least Relevant	Not Relevant
Least mportant	Not Important	Very Important	Important

Not Relevant	Least Relevant	Very Relevant	Relevant
Very Important	Important	Not Important	Least Important

A. Gap Analysis - Implementation Extent

The purpose of this section was to find out the implementation relevance of the different security controls from selected experts. The numbers in brackets next to the questions in table 5.7 to 5.8 represent the different security controls tested for this study. As mentioned earlier in section 4.3, the ISO/IEC 27000 family of standard is not implemented in Namibian organisations however organisations might still use the different security controls without following the ISO/IEC 27001 framework. The questions below were used to measure the relevance and importance of security controls in organisations:

- ✓ How relevant are the factors below in the implementation of the ISO/IEC 27000 family of standards in your organisation?

- ✓ Which factors are important in the implementation of the ISO/IEC 27000 family of standards in Namibia?

As explained in the theoretical framework evaluation section, the evaluated sections have matching and contradicting responses. Table 1 and 2 in Appendix E displays the findings for all 11 respondents for the security controls relevance and importance.

Four respondents had matching responses for all their choices and respondent number 1 and 11 had one contradicting choice. The other five had the highest contradicting responses: respondent 2 had 12 contradicting responses, respondent 4 had 7 contradicting responses, respondent 5 had 17 contradicting responses, respondent 9 had 12 contradicting responses and respondent 10 had 11 contradicting responses. The four respondents with all matching results show that they understood the questions. The other respondent showed that either the participants didn't understand the question or they were not reading the questions properly. Different choices for all 11 respondents are in the Microsoft excel document IEC 27000 Standards Implementation in Namibia Response Validation.xlsx.

Most participants indicated that the implementation of ISO/IEC 27000 family of standards security controls in their organisations is very relevant or relevant as depicted in table 3 in Appendix E. According to table 4 in Appendix E, most participants indicated that it is very important or important to implement the ISO/IEC 27000 family of standards security controls in Namibian organisations.

As explained earlier, this section had two similar questions evaluating the relevance and importance of the security controls. To come up with a total percentage for each security controls tested the percentages for the choices in table 3 and 4 in Appendix E were added and divided by two as follows:

- ✓ **Total Very Important (TVI)** = (very relevant (VR) + very important(VI))/2
- ✓ **Total Important (TI)** = (relevant (R) + important (I))/2
- ✓ **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- ✓ **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.7 displays the results of the total security controls percentages.

Table 5.7 Total matching response and percentage importance

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
1. Regularly reviewed Information Security policies (5.1.1- 5.1.2)	100	67	83.5	0	33	16.5	0	0	0	0	0	0
2. Policy governing removable IT media (8.3.1)	78	44	61	22	56	39	0	0	0	0	0	0
3. Formal procedure governing how removable IT media is disposed (8.3.2)	62.5	37.5	50	37.5	62.5	50	0	0	0	0	0	0
4. Documented and communicated access control policy based on business requirements (9.1.1)	73	45	59	27	55	41	0	0	0	0	0	0
5. Communicated policy document covering the organisations practices in how secret authentication information must be handled (9.3.1)	89	56	72.5	11	44	27.5	0	0	0	0	0	0
6. Policy on the use of cryptographic controls (e.g. encryption and	67	67	67	33	33	33	0	0	0	0	0	0

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
decryption of information) (10.1.1)												
7. Processes to detect and prevent malware (12.2.1)	91	64	77.5	9	36	22.5	0	0	0	0	0	0
8. Process and capacity to recover from a malware infection (12.2.1)	80	70	75	20	30	25	0	0	0	0	0	0
9. Agreed backup policy that complies with relevant legal frameworks (12.3.1)	91	64	77.5	9	36	22.5	0	0	0	0	0	0
10. Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)	100	87.5	93.75	0	12.5	6.25	0	0	0	0	0	0
11. Appropriate event logs and sysadmin / sysop logs maintained and reviewed? (12.4.1-12.4.3)	86	71	78.5	14	29	21.5	0	0	0	0	0	0
12. Managers who are regularly	56	44.4	50.2	22	33.3	27.65	22	11.1	16.55	0	11.1	5.55

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
instructed to review compliance with policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)												
13. Organisational policies that govern how information is transferred? (13.2.1)	87.5	75	81.25	12.5	25	18.75	0	0	0	0	0	0
14. Information security function with documented, implemented validated, verified and maintained processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)	100	71	85.5	0	29	14.5	0	0	0	0	0	0
15. Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)	86	43	64.5	14	57	35.5	0	0	0	0	0	0

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
16. Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)	100	62.5	81.25	0	37.5	18.75	0	0	0	0	0	0
17. Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)	70	50	60	10	40	25	0	10	5	20	0	10
18. Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)	80	60	70	0	20	10	0	0	0	20	20	20
19. Formal disciplinary process which allows the organization to take action against	78	33	55.5	22	67	44.5	0	0	0	0	0	0

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
employees who have committed an information security breaches (7.2.3)												
20. Formal disciplinary process communicated to all employees (7.2.3)	87.5	37.5	62.5	12.5	62.5	37.5	0	0	0	0	0	0
21. Documented process for terminating or changing employment duties relate to information security (7.3.1)	100	71	85.5	0	29	14.5	0	0	0	0	0	0
22. Background verification checks carried out on all new employees? (7.1.1)	56	57	56.5	22	14	18	22	29	25.5	0	0	0
23. Employees, contractors and third-party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)	78	56	67	22	44	33	0	0	0	0	0	0
24. Are managers (of	75	50	62.5	25	50	37.5	0	0	0	0	0	0

Security Controls	Number of responses per category											
	VI %	VR %	TVI %	I	R	TI%	NI	NR	TNI %	LI	LR	TLI %
all levels) engaged in driving security within the business? (7.2.1)												
25. Process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role? (9.2.5 - 9.2.6)	91	73	82	9	27	18	0	0	0	0	0	0

The numbers in brackets next to the questions in table 5.7 represent the different security controls from the ISO/IEC 270001 tested for this study. Table 5.8 depicts the different security controls tested for this study and their very important and important results. The results show the number of responses per security control. The researcher selected security controls that deal directly with information security. Most participants said the security controls are very important or important to be implemented in Namibian organisations.

Table 5.8 Results of different security controls

Security controls	Number of responses per category (%)	
	Very Important	Important
1. 5.1.1 – Policies for information 5.1.2 – Review of the policies for information security	83.5	16.5
2. 8.3.1- Management of removable media	61	39

Security controls	Number of responses per category (%)	
	Very Important	Important
3. 8.3.2 - Disposal of media	50	50
4. 9.1.1 - Access control policy	59	41
5. 9.3.1- Use of secret authentication information	72.5	27.5
6. 10.1.1 Policy on the use of cryptographic controls	67	33
7. 12.2.1 - Controls against malware	77.5	22.5
8. 12.2.1- Controls against malware	75	25
9. 12.3.1 - Information backup	77.5	22.5
10. 12.4.2 Protection of log information	93.75	6.25
11. 12.4.1- Event logging 12.4.3 - Administrator and operator logs	78.5	21.5
12. 18.2.1 - Independent review of information security 18.2.2 - Compliance with security policies and standards	50.2	27.65
13. 13.2.1 - Information transfer policies and procedures	81.25	18.75
14. 17.1.2 Implementing information security continuity 17.1.3 Verify, review and evaluate information security continuity	85.5	14.5
15	64.5	35.5

Security controls	Number of responses per category (%)	
	Very Important	Important
8.3.3 - Physical media transfer		
16. 13.2.3 - Electronic messaging	81.25	18.75
17. 9.2.1 – User registration and de-registration 9.2.2 - User access provisioning	60	25
18. 7.2.2 - Information security awareness, education and training	70	10
19. 7.2.3 - Disciplinary process	55.5	44.5
20. 7.2.3 -Disciplinary process	62.5	37.5
21. 7.3.1 - Termination or change of employment responsibilities	85.5	14.5
22. 7.1.1 - Screening	56.5	18
23. 7.1.2 - Terms and conditions of employment	67	33
24. 7.2.1 - Management responsibilities	62.5	37.5
25. 9.2.5 – Review of user access rights 9.2.6 - Removal or adjustment of access rights	82	18

Figure 5.7 displays the tested security controls from ISO/IEC 27001, the control domains and control objectives and how they are grouped. For example the control domain communication security had one control objective (Information transfer) tested for this study and two security controls (Information transfer policies and procedures, and electronic messaging) under that security objectives.

Figure 5.7 ISO/IEC 27001 control domains, control objectives and controls

B. Security Landscape of Namibia

To determine the relevance and importance of the implementation extent of the ISO/IEC 27000 family of standards and the factors that affect the implementation of the standards, the question below was used:

- ✓ To understand the security landscape of Namibia, may you please rate the relevance of the following items in ensuring information security?

This section had three contradicting responses and they are as follows:

- ✓ Respondent 1 had one contradicting response
- ✓ Respondent 10 had two contradicting responses

Table 5 and 6 in Appendix E shows the results.

All participants with matching responses agreed that it is very relevant (50%) and relevant (50%) to determine the implementation extent of the standard. Determining the factors that affect the implementation of the standard was observed as very relevant (44.4%) and relevant (44.4%) when determining the security landscape of Namibia. Table 7 in Appendix E depicts the results.

Table 8 in Appendix E indicates that all matching responses showed that it is very important (100%) to determine the implementation extent of the standard and the factors that affect the implementation of the standard when determining the security landscape of Namibia.

This section had two similar questions evaluating the relevance and importance of the security landscape of Namibia. To come up with a total percentage for each factor under the security landscape of Namibia, the percentages for the choices in table 8 and 9 in Appendix E were added and divided by two as follows:

- **Total Very Important (TVI)** = (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.9 displays the results of the total percentages of the security landscape of Namibia.

Table 5.9 Security landscape of Namibia findings - Importance

	Number of responses per category											
	VI	**VR**	**TVI %**	**I**	**R**	**TI%**	**NI**	**NR**	**TNI%**	**LI**	**LR**	**TLI%**
Determining the implementation extent of the standard	100	50	75	0	50	25	0	0	0	0	0	0
Determining the factors that affect the implementation of the standard	100	44.4	72.2	0	44.4	22.2	0	0	0	0	11.1	5.6

The final results depict that most users agreed that it is very important (75%) and important (25%) to determine the implementation extent of the standard.

Almost all participants agreed that determining the factors that affect the implementation of the ISO/IEC 27000 family of standard is very important (72.2%) and important (22.2%). Only 5.6% said it is least important to determine the factors that affect the implementation of the standard. The final results are displayed in figure 5.8.

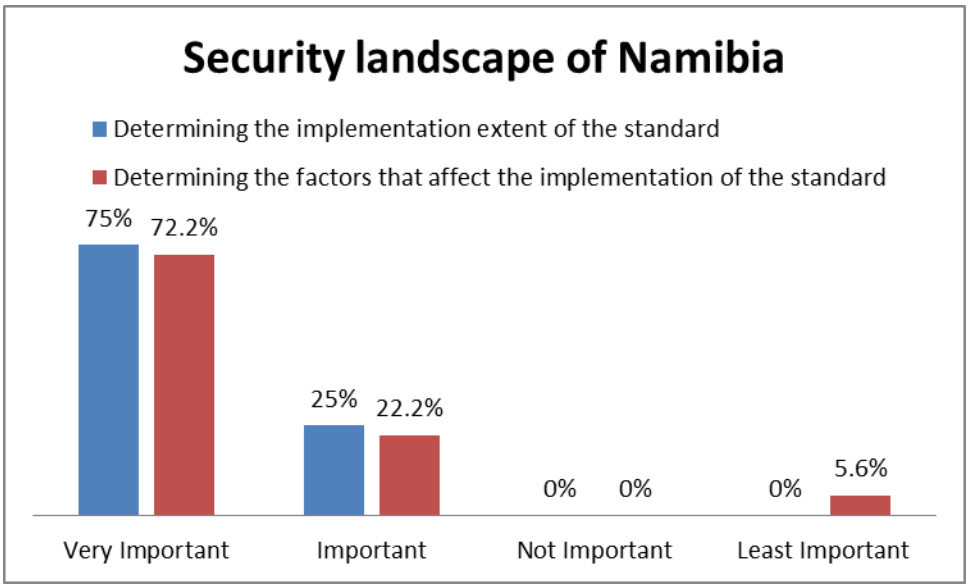


Figure 5.8 Final Results: Security landscape of Namibia

C. What is needed?

The purpose of this section was to determine the relevance and importance of what is needed to mitigate information security risks in organisations. The question below was used:

- ✓ What is needed to mitigate information security risks in your organisation?

One contradicting response was found in this section from respondent 1 and the results are depicted in table 9 and 10 in Appendix E.

The total percentages of matching responses were calculated and they are shown in table 11 and 12 in Appendix E. All matching responses agreed that it is very relevant (81.8%) and relevant (18.18%) and that an in-depth study of the standard is performed to determine what is needed to mitigate information security risks in organisations (see table 11 in Appendix E). They also agreed that the development of national adoption policy frameworks is very relevant (90%) and relevant (10%) (see table 11 in Appendix E).

Table 12 in Appendix E shows that all matching responses agreed that it is very important (90.9%) and important (9.09%) that an in-depth study of the standard is performed to determine what is needed to mitigate information security risks in organisations. All respondents said that the development of a national adoption policy framework is very important (90%) and important (10%) to mitigate information security risks.

This section had two similar questions evaluating the relevance and importance of what is needed to mitigate information security risks in Namibian organisations. To come up with a total percentage for each determining factor of what is needed to mitigate information security risks, the percentages for the choices in table 11 and 12 in Appendix E were added and divided by two as follows:

- **Total Very Important (TVI)** (= (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.10 displays the results of the total percentages of what is needed to mitigate information security risks in Namibian organisations.

Table 5.10 What is needed - Total percentage of matching responses

	Number of responses per category											
	VI	**VR**	**TVI %**	**I**	**R**	**TI%**	**NI**	**NR**	**TNI%**	**LI**	**LR**	**TLI%**
Extensive/in-depth study of the standard	90.9	81.8	86.35	9.09	18.18	13.64	0	0	0	0	0	0
Development of national adoption policy frameworks	90	90	90	10	10	10	0	0	0	0	0	0

The final results shown in figure 5.9 depict that all respondents agreed that it is very important (86.35%) and important (13.64%) to perform an in-depth study of the standard. The development of national adoption policy frameworks was also agreed as a very important (90%) and important (10%) factor in mitigating information security risks.

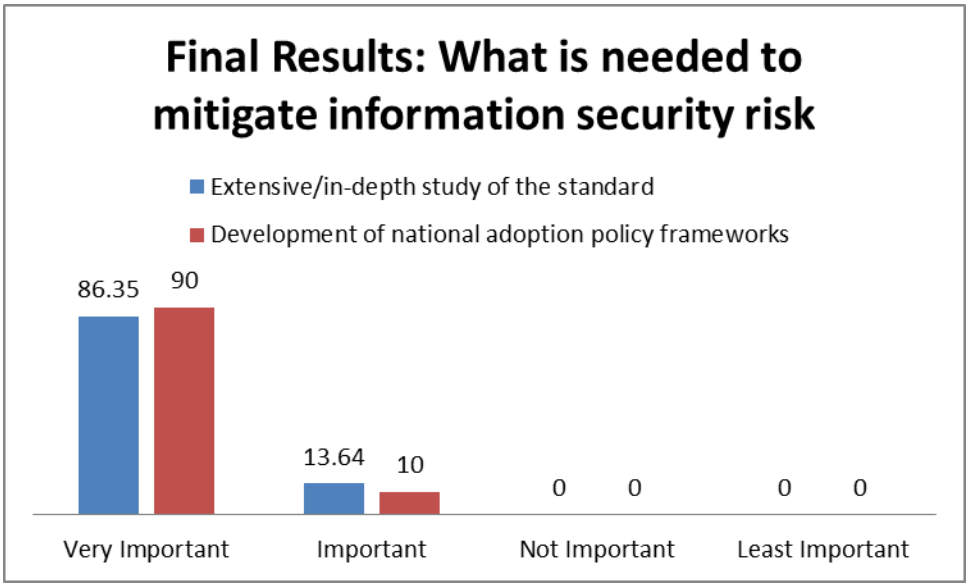


Figure 5.9 Final Results: What is needed to mitigate information security risk

D. Mitigating Strategy

This section evaluated the relevance and importance of the implementation or adoption of ISO/IEC 27000 family of standards framework as an information technology mitigating strategy. The questions below were used:

- To what extent is this relevant for information security risk mitigation?
- To what extent is this important for information security risk mitigation?

This section had no contradicting responses (see table 13 and 14 in Appendix E).

The results revealed that all respondents agreed that the implementation or adoption of ISO/IEC 27000 family of standards framework is very relevant (63.6%) and relevant (36.4%) as the information security risk mitigating strategy. The results are depicted in table 15 in Appendix E.

The importance of the implementation or adoption of ISO/IEC 27000 family of standards framework as the information security risk mitigating strategy was also tested and the respondents agreed that it is very important (90.9%) and important (9.1%) as depicted in table 16 in Appendix E.

This section had two similar questions evaluating the relevance and importance of the implementation or adoption of ISO/IEC 27000 family of standards framework as the information security risk mitigating strategy in Namibian organisations. To come up with a total percentage of the mitigating strategy, the percentages for the choices in table 15 and 16 in Appendix E were added and divided by two as follows:

- **Total Very Important (TVI)** (= (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.11 displays the results of the total percentages of the implementation or adoption of ISO/IEC 27000 family of standards framework as the information security risk mitigating strategy in Namibian organisations.

Table 5.11 Mitigating strategy - Total percentage of matching responses

	Number of responses per category											
	VI	**VR**	**TVI %**	**I**	**R**	**TI%**	**NI**	**NR**	**TNI%**	**LI**	**LR**	**TLI%**
Implementation or adoption of ISO 27000 family of standard framework	90.9	63.6	77.25	9.1	36.4	22.75	0	0	0	0	0	0

The final results depict that it is very important (77.25%) and important (22.75%) to implement or adopt the ISO/IEC 27000 family of standards framework as an information security mitigating strategy. The results are depicted in figure 5.10.

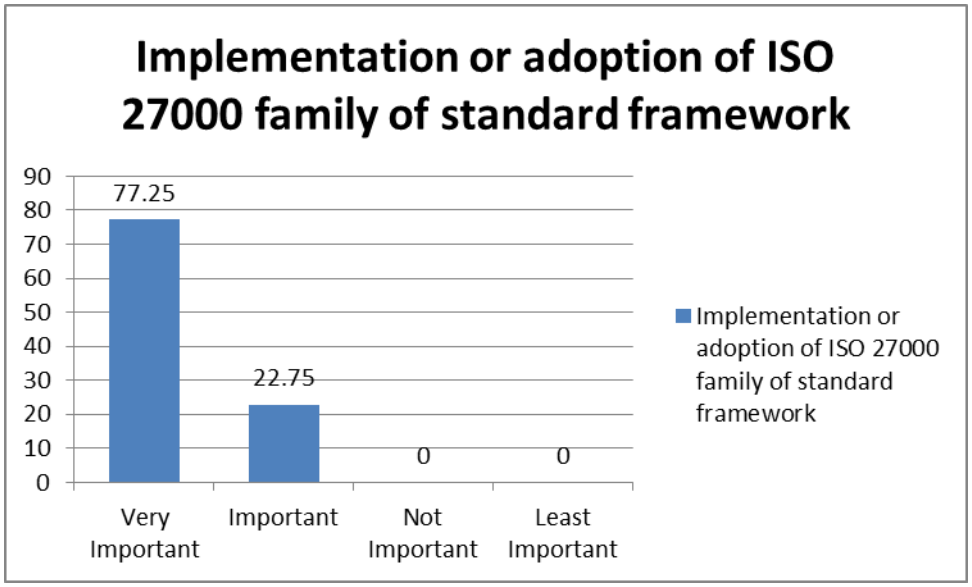


Figure 5.10 Final Results: Mitigating strategy

E. Factors Affecting the Adoption of ISO/IEC 27000 Standards

This section intended to evaluate the relevance and importance of the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibian organisations. The statement below was used:

- ✓ Factors affecting the adoption of ISO/IEC 27000 Standards

This section had 10 contradicting responses from 4 respondents and the results are depicted in table 17 and 18 in Appendix E and they are as follows:

- Respondent 1 had one contradicting response
- Respondent 3 had one contradicting response
- Respondent 9 had five contradicting responses
- Respondent 10 had three contradicting responses

The contradicting responses show that the respondent did not understand the questions or did not read it properly. The results reveal that almost all respondents agreed that the factors affecting the adoption of the ISO/IEC 27000 family of standards were either very relevant and relevant or very important and important. The factors that were evaluated by the participants are listed in table 19 and 20 in Appendix E, together with a percentage measure for each factor. Table 5.12 display the results of the matching responses only.

This section had two similar questions evaluating the relevance and importance of the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibian organisations. To come up with a total percentage of the mitigating strategy, the percentages for the choices in table 19 and 20 were added and divided by two as follows:

- **Total Very Important (TVI)** (= (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.12 displays the results of the total percentages of the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibian organisations.

Table 5.12 Factors affecting the adoption of the standard - Total percentage of matching responses

	Number of responses per category											
	VI	VR	TVI %	I	R	TI%	NI	NR	TNI%	LI	LR	TLI%
Technical team experience	90	70	80	10	30	20	0	0	0	0	0	0
Deployment of the right IT personnel	80	80	80	20	20	20	0	0	0	0	0	0
Willingness to change	75	87.5	81.25	25	12.5	18.75	0	0	0	0	0	0
Clear understanding of standards	80	70	75	20	30	25	0	0	0	0	0	0
Top management involvement	80	80	80	20	20	20	0	0	0	0	0	0
Organisational information security Culture	81.82	72.73	77.28	9.09	18.18	13.64	0	0	0	9.09	9.09	9.09
Employees lack of discipline towards information security	100	54.55	77.28	0	36.36	18.18	0	0	0	0	9.09	4.55
Improper Information Security documentation	90.91	63.64	77.28	9.09	36.36	22.73	0	0	0	0	0	0

	Number of responses per category											
	VI	VR	TVI %	I	R	TI%	NI	NR	TNI%	LI	LR	TLI%
Inadequate IT budget	87.5	50	68.75	12.5	30	21.25	0	0	0	25	20	22.5
Identifying organisation's IT assets	90.91	81.82	86.37	9.09	18.18	13.64	0	0	0	0	0	0
Appropriate enforcement of IT policies and procedures	88.89	77.78	83.34	11.11	22.22	16.67	0	0	0	0	0	0

The final results reveal that the factors affecting the adoption of the ISO/IEC 27000 family of standards are mostly very important and important as depicted in figure 5.11.

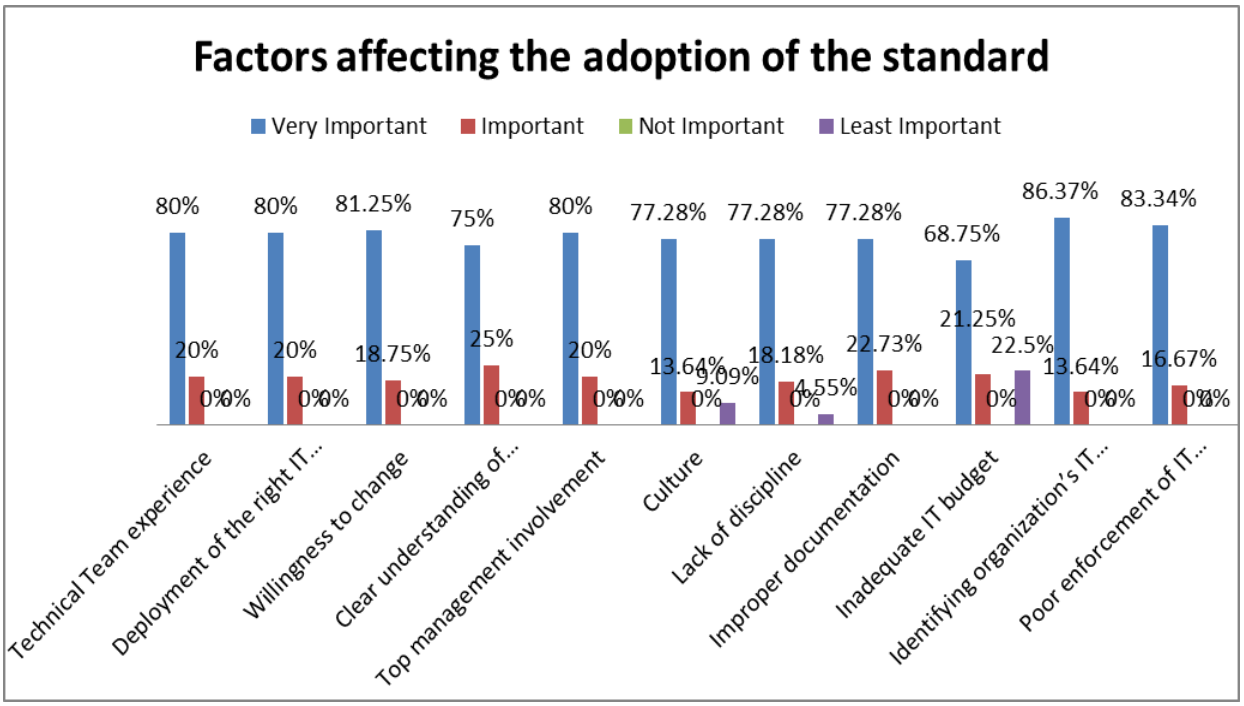


Figure 5.11 Factors affecting the adoption of the standard

F. Benefits of Implementing ISO/IEC 27000 Family of Standards

The purpose of this section was to evaluate the relevance and importance of the benefits of implementing ISO/IEC 27000 family of standards in Namibian organisations. The statement below was used:

- ✓ Benefits of implementing ISO 27000 family of standards

This section had one contradicting response from respondent one. See results in table 21 and 22 in Appendix E.

Almost all participants agreed that the benefits of implementing ISO/IEC 27000 family of standards listed in table 23 and 24 in Appendix E are either very relevant and relevant, or very important and important.

This section had two similar questions evaluating the relevance and importance of the benefits of implementing ISO/IEC 27000 family of standards in Namibian organisations. To come up with a total percentage of the ISO 27000 family of standards benefits, the percentages for the choices in table 23 and 24 were added and divide by two as follow:

- **Total Very Important (TVI)** (= (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.13 displays the results of the total percentages of the benefits of implementing ISO/IEC 27000 family of standards in Namibian organisations.

Table 5.13 Benefits of implementing ISO/IEC 27000 family of standards - Total percentage of matching responses

	Number of responses per category											
	VI	VR	TVI %	I	R	TI%	NI	NR	TNI%	LI	LR	TLI%
Protect crucial resources	90.91	90.91	90.91	9.09	9.09	9.09	0	0	0	0	0	0
Managing risks more efficiently	81.82	72.73	77.28	18.18	27.27	22.73	0	0	0	0	0	0
Improving and maintaining customer confidence	80	60	70	20	40	30	0	0	0	0	0	0
Benchmarking to international best practices	63.64	63.64	63.64	36.36	36.36	36.36	0	0	0	0	0	0
Avoid brand damage and change its information security posture alongside technological developments	72.73	63.64	68.19	18.18	27.27	22.73	9.09	9.09	9.09	0	0	0

The final results depict that almost all respondents agreed that the ISO 27000 family of standards benefits are very important and important except for one user who said of the benefit: “Avoid brand damage and change its information security posture alongside technological developments” is not important. The results are displayed in figure 5.12.

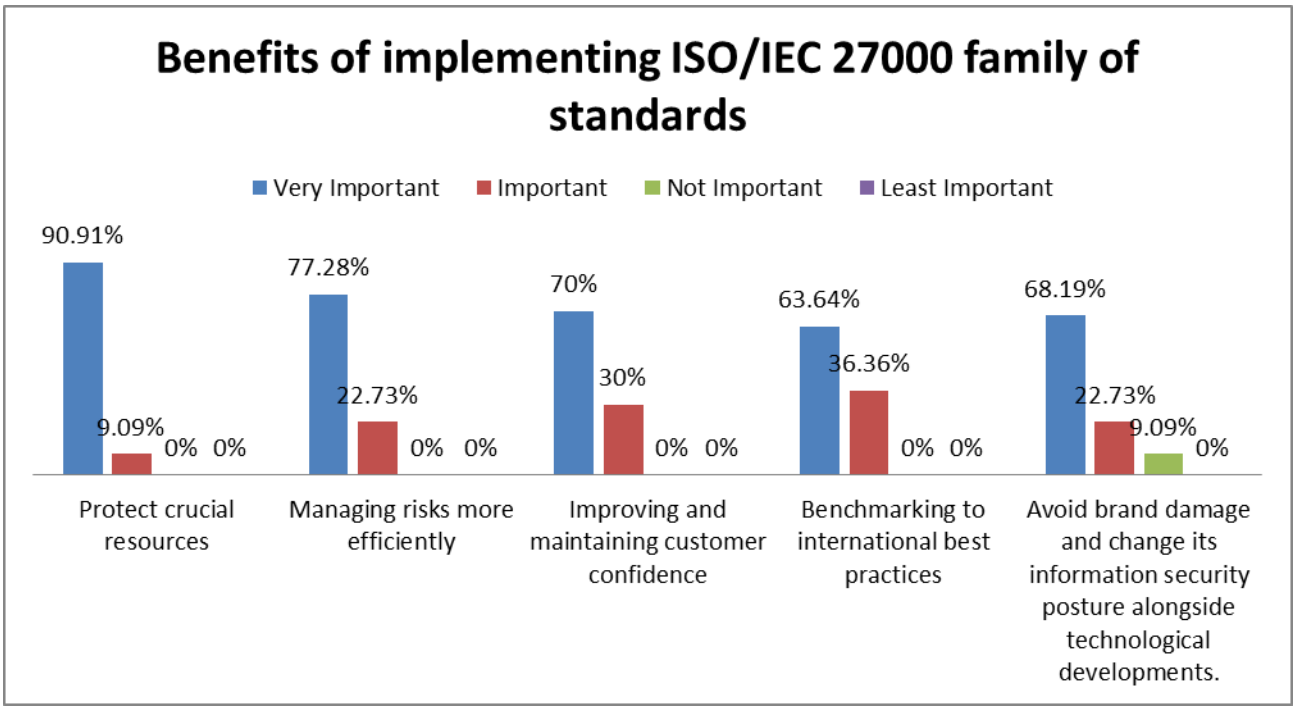


Figure 5.12 Benefits of implementing ISO/IEC 27000 family of standards

For the section any other comments in the evaluation tool, none of the respondents gave any comment.

G. Information Security Controls

This section aimed to evaluate the importance and relevance of security controls. The question below and the security controls listed in the tables under this section were used:

- ✓ Please rate the importance of the security controls

This section had one contradicting response from respondent number ten and the result is depicted in table 25 and 26 in Appendix E.

Almost all participants agreed that the security controls in table 27 and 28 in Appendix E are very important and important, or very relevant and relevant except for four respondents each saying that one of these four security controls namely operations security, cryptography, system acquisition, development and maintenance, and human resource security is least important and least relevant.

This section had two similar questions evaluating the relevance and importance of security controls. To come up with a total percentage of the security controls, the percentages for the choices in table 27 and 28 in Appendix E were added and divided by two as follows:

- **Total Very Important (TVI)** = (very relevant (VR) + very important(VI))/2
- **Total Important (TI)** = (relevant (R) + important (I))/2
- **Total Not Important (TNI)** = (not relevant (NR) + not important (NI))/2
- **Total Least Important (TLI)** = (least relevant (LR) + least important (LI))/2

Table 5.14 displays the results of the total percentages of the security controls.

Table 5.14 Security Controls - Total percentage of matching responses

	Number of responses per category											
	VI	VR	TVI %	I	R	TI%	NI	NR	TNI%	LI	LR	TLI%
Information Security Policies	90.91	72.73	81.82	9.09	27.27	18.18	0	0	0	0	0	0
Operations Security	63.64	63.64	63.64	27.27	27.27	27.27	0	0	0	9.09	9.09	9.09
Cryptography	36.36	45.45	40.91	54.55	45.45	50	0	0	0	9.09	9.09	9.09
System acquisition, development and maintenance	54.55	72.73	63.64	36.36	18.18	27.27	0	0	0	9.09	9.09	9.09
Asset Management	63.64	45.45	54.55	36.36	54.55	45.455	0	0	0	0	0	0
Human Resource Security	72.73	36.36	54.55	18.18	54.55	36.365	0	0	0	9.09	9.09	9.09
Compliance	81.82	72.73	77.28	18.18	27.27	22.725	0	0	0	0	0	0
Access Control	100	81.82	90.91	0	18.18	9.09	0	0	0	0	0	0
Organisation of information security	100	81.82	90.91	0	18.18	9.09	0	0	0	0	0	0
Communication Security	90	100	95	10	0	5	0	0	0	0	0	0

The final results depict that respondents agreed that 6/10 security controls are 100% very important and important, namely information security policies, asset management, compliance, access control, organisation of information security and communication security.

Respondents also agreed that the other four security controls namely operations security, cryptography, system acquisition, development and maintenance, and human resource security are very important and important expect for four respondents, each saying that one of the four security controls is least important. The results are displayed in figure 5.13.

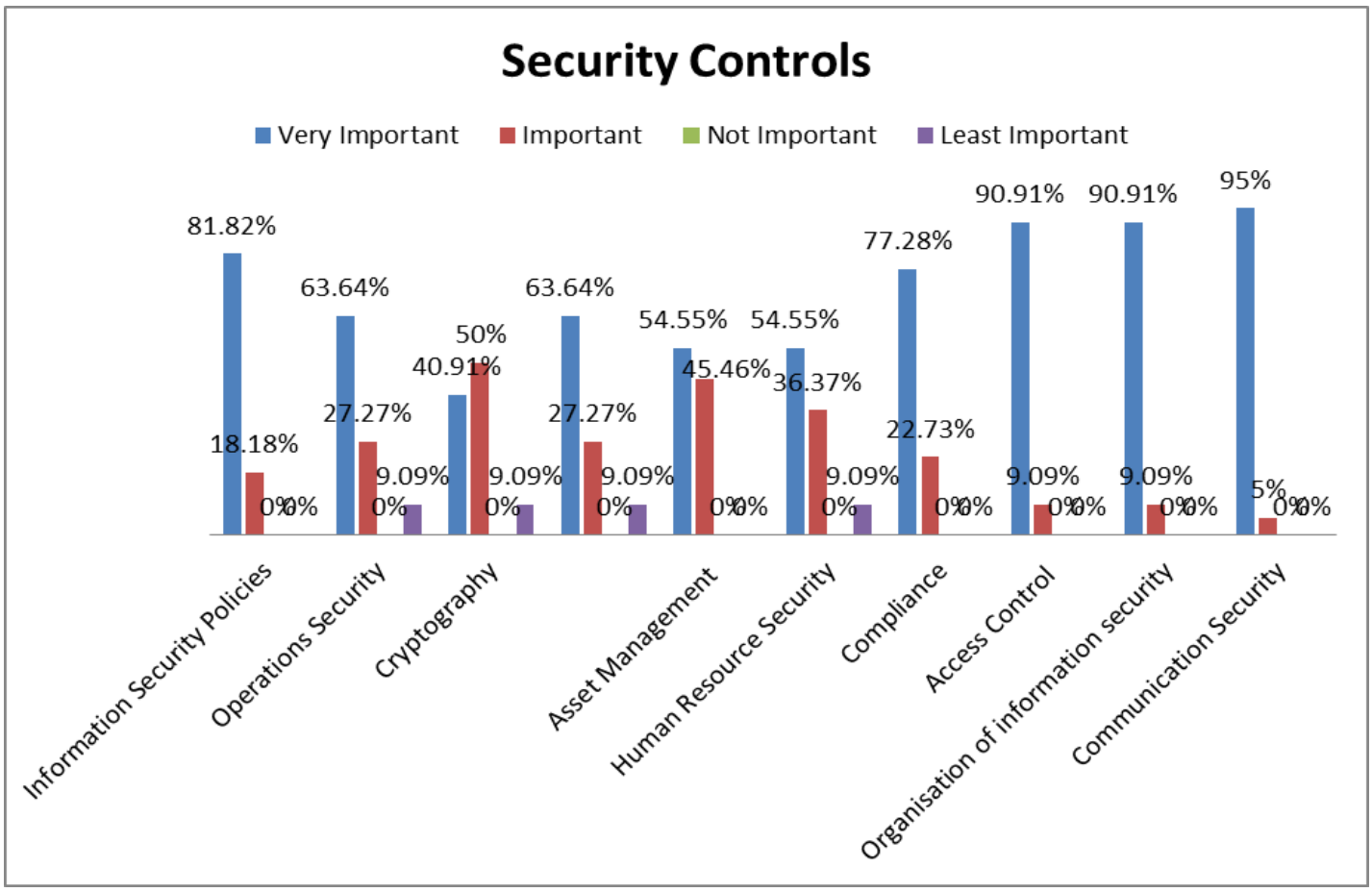


Figure 5.13 Security Controls

H. Overall Framework Evaluation

The purpose of this section was to validate the whole theoretical framework. The question below was used to validate the overall framework:

- Please validate the whole theoretical framework - To what extent is the presented theoretical framework as a whole meeting the following criteria?

The respondents rated the extent of the framework criteria as follows:

Efficient – 90% of participants strongly agreed and agreed that the framework is efficient, while 10% disagreed that the framework is efficient.

Operational – 100% of the participants strongly agreed and agreed that the framework is operational.

Well designed and developed - 90% of participants strongly agreed and agreed that the framework is well designed and developed, while 10% disagreed that the framework is well designed and developed.

Relevant and needed - 100% of the participants strongly agreed and agreed that the framework is relevant and needed.

Useful and valuable - 100% of the participants strongly agreed and agreed that the framework is useful and valuable.

Adaptable and customisable - 100% of the participants strongly agreed and agreed that the framework is adaptable and customisable.

Requires a lot of improvement - 63.63 strongly agreed and agreed that the framework requires a lot of improvement while 36.36 strongly disagreed and disagreed that the framework requires a lot of improvements.

Table 5.15 and figure 5.14 display the results depicted above.

Table 5.15 Overall Framework Evaluation - Total percentage responses

	Number of responses per category								
	Total Response	**Strongly Agree**	**%**	**Agree**	**%**	**Disagree**	**%**	**Strongly Disagree**	**%**
Efficient	10	5	50	4	40	1	10	0	0
Operational	10	4	40	6	60	0	0	0	0

Well designed and developed	10	3	30	6	60	1	10	0	0
Relevant and needed	10	6	60	4	40	0	0	0	0
Useful and valuable	10	8	80	2	20	0	0	0	0
Adaptable and customisable	10	5	50	5	50	0	0	0	0
Requires a lot of improvement	11	5	45.45	2	18.18	3	27.27	1	9.09

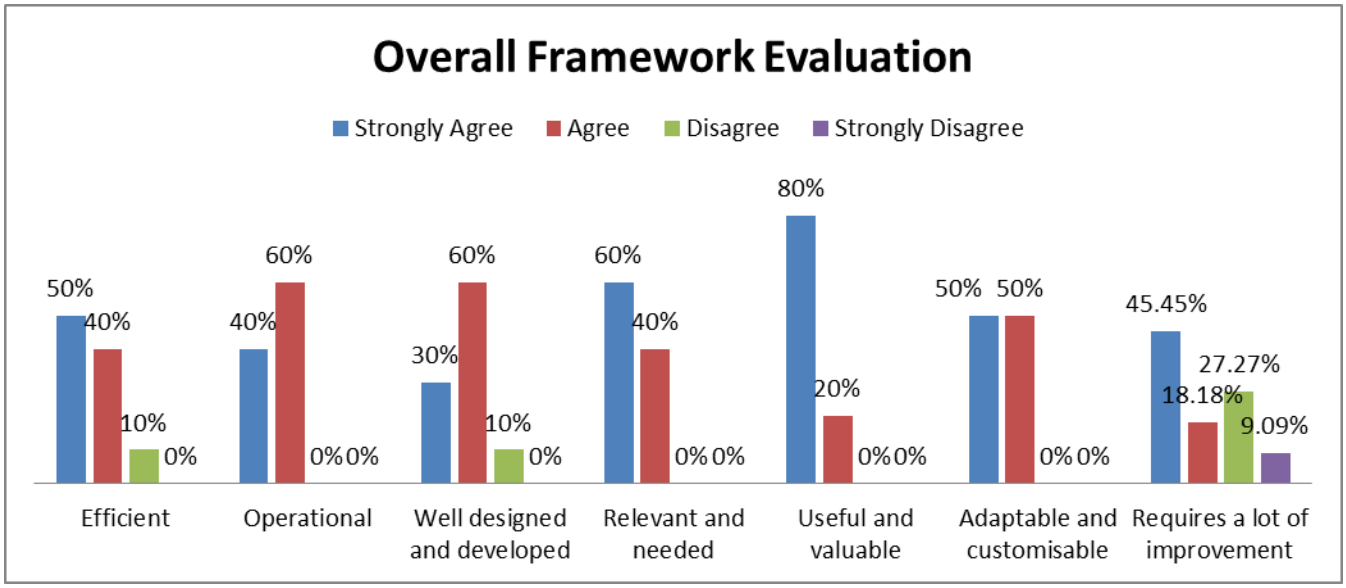


Figure 5.14 Overall Framework Evaluation

For the section any other comments in the evaluation tool, none of the respondents gave any comment.

5.6.5 Summary of Findings

The importance and relevance of the sections above were evaluated and the summary is presented below:

Gap analysis implementation extent of security controls – Almost all participants agreed that the implementation of the ISO/IEC 27000 family of standards security controls in organisations is very important and important.

Security landscape of Namibia – Almost all participants agreed that the factors determining the extent of Namibia's security landscape are very important and important.

What is needed – Almost all participants agreed that it is very important and important to perform an in-depth study of the standard and develop a national adoption policy framework to mitigate information security risks in organisations.

Mitigation strategy – All participants agreed that it is very important and important to implement or adopt the ISO/IEC 27000 family of standards framework as an information security mitigating strategy.

Factors affecting the adoption of ISO/IEC 27000 Standards – Almost all participants agreed that the factors affecting the adoption of the ISO/IEC 27000 family of standards are very important and important.

Benefits of implementing ISO 27000 family of standards – Almost all participants agreed that the ISO 27000 family of standards benefits are very important and important.

Information security controls - Respondents agreed that 6/10 security controls are 100% very important and important and the other four security controls are mostly very important and important.

Evaluation of the whole theoretical framework – All participants agreed that the framework is 100% operational, relevant and needed, useful and valuable, and adaptable and customisable. The framework was also said to be 90% efficient and well designed and developed. More than half of the participants (63.63%) strongly agreed and agreed that the framework requires a lot of improvements. The other 36.36% strongly disagreed and disagreed that the framework requires a lot of improvements.

The next section will discuss the framework communication process.

5.7 Communication

The framework was communicated at the IST Africa conference for peer-reviewing and publication. The framework was also communicated to selected stakeholders and experts to evaluate the relevance of the framework components, and the framework itself. And finally, the framework is presented as part of this thesis.

The results of the theoretical framework evaluation in section 5.6.2.1 depicted that almost all participants agreed that the theoretical framework is operational, relevant and needed, useful and valuable, and adaptable and customisable. More than half of the participants (63.63%) strongly agreed and agreed that the framework requires a lot of improvements. The other 36.36% strongly disagreed and disagreed that the framework requires a lot of improvement. Participants who indicated that the framework requires a lot of improvement didn't specify the improvements to be made on the framework. The framework was refined and it's presented in figure 5.15. An explanation of the ISO/IEC 27000 family of standards national adoption policy framework is provided in section 5.7.1 to provide clarity on the framework.

Since almost all participants agreed with the theoretical framework components and the framework itself, the framework was refined and an ISO/IEC 27000 family of standards national adoption policy framework was designed as shown in figure 5.14. The ISO/IEC 27000 family of standards national adoption policy framework is very important to mitigate information security risks in Namibian organisations. The information security policy structure components are discussed in section 5.7.1.

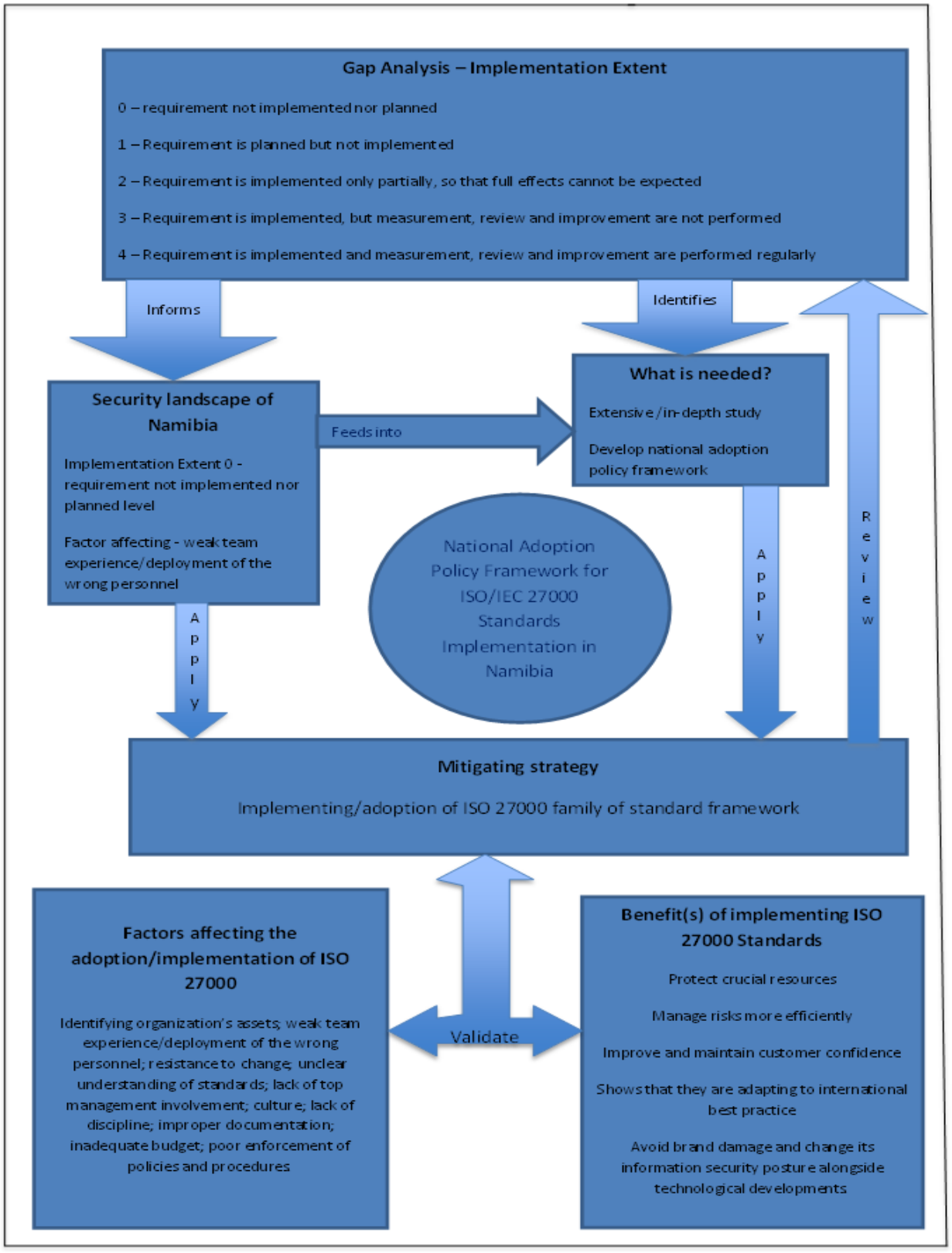


Figure 5.15 National Adoption Policy Framework for ISO/IEC 27000 Standards Implementation

5.7.1 Information Security Policy

Information security policy structure components presented in section 2.7.2 are important for an information security policy. The national adoption policy framework for ISO/IEC 27000 standards implementation for Namibia consist of the following information security policy structures: introduction, purpose, objectives, scope, responsibilities, rights and duties of personnel, monitoring and evaluation and specific instructions and they are described below.

5.7.1.1 Introduction

The national adoption policy framework for ISO/IEC 27000 standards implementation was designed for organisations in Namibia to help mitigate information security risks. The framework has different components that will assist information security experts with the standard implementation, namely gap analysis, security landscape, mitigating strategy, factors affecting the adoption and implementation, and benefit of implementing ISO/IEC 27000 family of standards.

5.7.1.2 Purpose

The aim of this framework is to set out the adoption of the ISO/IEC 27000 family of standards as an information security mitigating strategy.

5.7.1.3 Objectives

The framework set out the benefits of implementing ISO/IEC 27000 as guidance for management and information security experts when implementing the standard.

5.7.1.4 Scope

This policy framework applies to all organisations in Namibia who will implement the ISO/IEC 27000 family of standards.

5.7.1.5 Responsibilities, rights and duties of personnel

This specifies the structure of employees' responsibilities, rights and duties for the policy implementation. The information of selected stakeholders for this study are listed in section 5.6.2.1 (biographical information).

5.7.1.6 Monitoring and evaluation

The standard implementation extent, the steps used to determine the implementation extent and the risk management strategy are part of the framework. This section lists the steps to determining the factors affecting the adoption/implementation of the ISO/IEC 27000 family of standards in Namibian organisations. Auditing of information security risks for security controls is listed under this section - see figure 5.7 for the security controls used for this study.

5.7.1.7 Specific instructions

To mitigate information security risks in Namibian organisations, an extensive or in-depth study of the ISO 27000 family of standards and the development of the standard is important.

5.8 Summary

The chapter discussed the design of a national adoption policy framework for ISO/IEC 27000 family of standards for Namibian organisations which followed the six phases of design science research by Peffers et al. (2008). The problem identification and motivation discussed the study's problem and how the problem would be solved. A definition of the objectives for a solution stage listed the study's objectives and what the framework will achieve. The design and development phase presented the theoretical framework design and the framework implementation guideline. The demonstration phase shows an example of an ISO/IEC 27000 family of standards policy. The evaluation phase presented the theoretical framework evaluation pilot study and evaluation tool results. The communication phase discussed the refined framework.

The next chapter is the conclusion of the study and it also provides recommendations for future research.

Chapter 6 - Conclusions

6.1 Introduction

The previous chapters discussed the study's problem, literature reviews relevant to the study, methodologies, data collected for the study and the results and framework design process. This chapter gives a brief summary of the entire research study. Section 6.2 provides the research overview, section 6.3 discusses the research contribution, section 6.4 discusses the study's limitation, section 6.5 discusses the possible future research grounded from this study and section 6.6 summarises this chapter.

6.2 Overview of the Study

This study started off by reviewing literature sources about the phenomenon being studied, namely the ISO/IEC 27000 family of standards and these keywords were used: Information security, Information Security Management System, Information Security Policies, Policy framework and ISO/IEC 27000 series. Preliminary interviews were conducted with selected stakeholders. The research overview, problem statement, purpose of the study, research objectives, research questions and the significance of the study were derived from the literature and preliminary interviews, and they were discussed in chapter 1. Literatures relevant to the study were discussed in chapter 2. Research methodologies used to answer the research questions and meet the research objectives were discussed in chapter 3. Table 6.1 displays the research questions, research objectives, sampling methods and data collection methods used for this study.

Table 6.1 Research questions, research objectives, sampling methods and data collection methods

Questions	Objectives	Sampling Methods	Data collection Methods
What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?	Investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia	Purposeful sampling	- Case study - Literature review - Interview - Questionnaire
What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?	Investigate the factors affecting the adoption of ISO/IEC 27000 family of standards	Purposeful sampling	- Case study - Literature Review - Interview - Questionnaire – Expert Review
Main Research question How can a policy framework be constituted to guide the adoption of ISO/IEC 27000 family of standard into security practice?	**Main research objectives** Design a policy framework to guide the adoption of ISO/IEC 27000 security standards in the practice	Purposeful sampling	- Case study - Literature review - Design science methodology - Design and development stage

The preliminary interviews aimed to investigate the implementation extent of the ISO/IEC 27000 family of standards and to investigate the factors affecting the adoption of the standards and this was discussed in chapter 4. A gap analysis was applied on the collected data and it was depicted that the ISO/IEC 27000 family of standards is not implemented in Namibian organisations; however, there is consideration when the cyber security bill is gone through parliament. ISO/IEC 27000 policy adoption framework will guide the adoption of the ISO/IEC 27000 family of standards in Namibia.

Argumentation from literatures and the results from the preliminary interviews were used to design a theoretical framework presented in section 4.4. A framework evaluation tool was developed and a pilot study was conducted with master's students from the Namibia University of Science and Technology. Minor changes were recommended and amendments were done by the researcher. The theoretical framework was then evaluated by experts from the industry and academic institutions to evaluate whether the theoretical framework is operational, relevant and needed, useful and valuable, and adaptable and customisable. The importance of the ISO/IEC 27001 security controls and the validity of the framework components were also evaluated. Almost all experts agreed with the components of the theoretical framework. The framework was refined and a national adoption policy framework was designed and it is discussed in chapter 5.

6.3 Research Contributions

The problem of this study was identified as the usage and adoption of the ISO/IEC 27000 standards which is missing in Namibian organisations. The study aimed to design a national adoption policy framework for ISO/IEC 27000 family of standards for Namibia to help with the implementation and adoption of the standards as a way to gain the standard benefits and mitigate information security risks in Namibian organisations. This study has added to the body of knowledge of information security governance and risk management as a subset of information security on how a framework can enhance the mitigation of information security risks and to reduce the probability of information loss through a guided adoption process. This study identified the implementation extent of the ISO/IEC 27000 family of standards in Namibian organisations and it was established that Namibia is at 0 – requirement not implemented nor planned stage (see section 4.3).

The factors affecting the adoption of ISO/IEC 27000 family of standards in Namibian organisations were also identified as weak team experience or deployment of the wrong personnel as gleaned via a survey and this was supported by the literature as indicated in sections 4.2 and 4.3. Finally, implementation guidelines for the ISO/IEC 27000 policy adoption framework were designed and presented in chapter 5 to aid the adoption process.

6.4 Limitations

Although this research study reached its objectives and the research questions were answered, there were limitations. A cross sectional study was conducted which was limited to a case analysis of identified stakeholders to implement an ISO/IEC 27000 policy framework for security standards in Namibia. A longitudinal study should be conducted with Namibian organisations to allow for the generalisability of the framework. Several literatures were studied on the standards used elsewhere but the policy framework implemented is specific to Namibia. The lack of implementation of the framework is a study weakness; results of actual implementation would have shed light to its applicability and implication thereof.

6.5 Lesson Learnt

Many lessons are gained during a research project, academic as well as the non-academic. Academic lessons learnt during this research project are discussed.

When writing a thesis report, the chapters as well as the sections should be linked for the topics to flow, it is like writing a story; each chapter is distinct but yet they are linked.

The researcher's work needs to be reviewed by external parties for example at conference proceedings and research symposiums.

A broader knowledge of the ISO/IEC 27000 family of standards was also gained during the research project which enabled the researcher to meet the research project.

An immense interest in the area of information security governance was provoked and the researcher is aiming to advance in this area to protect Namibian organisations.
The thought of giving up comes and goes but with a good support you will make it.

6.6 Reflections

This section presents scientific, methodological and substantive reflections of this study.

6.6.1 Scientific Reflection

With more data stored electronically in these days rather than as hard copies, data needs to be protected to mitigate damage to organisations. Organisational damage can be experienced because of following information security issues: social engineering, unauthorized disclosure of information or passwords, access to the network by unauthorised persons, errors in maintenance, loss of electricity, human or natural disasters, malfunction of equipment, destruction of records, theft of hardware, fire, loss of productivity, financial loss, legal implications and organisational blackmail as presented in section 2.10. To mitigate information security risks, data needs to be governed and one standard used to mitigate information security risks is the ISO/IEC 27000 family of standards which was discussed in this thesis paper.

It was noticed through a preliminary interview conducted in 2015 that there is a poor/no implementation of the ISO/IEC 27000 family of standards in Namibian organisations while there are so many information security risks that can cause damage to organisations. The study designed a policy framework that guides the adoption of ISO/IEC 27000 family of standards into security best practices for Namibian organisations as presented in figure 5.14 of section 5.7. The designed national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia has added to the body of knowledge of information security governance and risk management as a subset of information security.

To guide the implementation of the national adoption policy framework for ISO/IEC 27000 standards, a framework implementation guideline was designed. The framework implementation guideline consists of the three components: Info Sec controls for ISO/IEC 27001 family of standards, ISMS pillars and information security pillars.

6.6.2 Methodological Reflection

The study aimed to investigate the implementation extent of the ISO/IEC 27000 framework adoption and the factors affecting the implementation of the standard in Namibia. A multi method qualitative research was used to collect and analyse the data. The data were collected using literature reviews to help understand the phenomenon, interviews to help determine the standard implementation extent and factors affecting the adoption of the standard and questionnaires to evaluate the theoretical framework. Content analysis was used to interpret and analyse the data to come up with a conclusion of the collected data.

This was realized using an exploratory case study strategy with selected stakeholders in Namibian organisations. This problem-based approach was used to come up with an artefact that can guide the adoption of ISO/IEC 27000 family of standards into security best practices for Namibian organisations using the DSRM method. The DSRM method used has six phases which were used to identify the problem and motivate the need for a research; define the study's objectives for a solution; the design and development of the theoretical framework; artefact demonstration and evaluation; and finally, the artefact communication as presented in Chapter 5.

6.6.3 Substantive Reflection

The study focused on designing a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia as an artefact using the DSRM method. The designed artefact belongs to the information security governance and risk management area within the information security field. To design the artefact, the study aimed to understand the implementation extent of the ISO/IEC 27000 family of standards, the factors affecting the adoption of the standard in Namibia and the following topics within the information security governance and risk management: information security governance, the ISO/IEC 27000 family of standards, gap analysis, theoretical framework, information security policy, ISMS pillars, information security pillars and the information security risk.

6.7 Possible Future Research

The national adoption policy framework for ISO/IEC 27000 standards implementation should be tested and implemented in a real-life environment in Namibia organisations to assist with mitigating information security risks and to reduce the probability of information loss. The framework implementation guideline was not tested for this study therefore, an evaluation tool should be designed to evaluate whether the framework implementation guideline is operational, adaptable and customisable. The evaluation needs to be conducted with information security experts from academic institutions and the industry. The ISO/IEC 27001 security standards use the PDCA cycle for a continuous improvement approach. The study focused on ISO/IEC 27001 clauses that fall under the plan phase of the PDCA cycle which involves establishing the ISMS. A future study should focus on establishing, implementing, operating, monitoring and reviewing of all ISO/IEC 27001 clauses using the PDCA cycle. This will assist with ensuring that an appropriate ISMS is implemented.

6.8 Conclusion

In conclusion, the main aim of the study was to address the set objectives: Table 6.2 gives a confirmation summary of the objectives achieved in this study.

Table 6.2 Research question, answers and evidence

Research Questions	Answer	Evidence
What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?	Namibian organisations are at level 0 – standards not implemented nor planned however there is a consideration when the Cyber Security Bill has been approved by parliament.	Section 4.3
What are the factors affecting the adoption of ISO/IEC 27000 family of standards in Namibia?	Weak team experience Deployment of the wrong personnel Employees are not trained and are not certified in ISO 27001	Section 4.3
Main Research question How can a policy framework be constituted to guide the adoption of ISO/IEC 27000 family of standard into security practice?	A national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia was designed. Framework implementation guidelines to aid with the framework implementation.	Chapter 5

THE END

REFERENCES

AbuSaad, B., Saeed, F.A., Alghathbar, K., & Khan, B. (2011). *Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned*. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1104&context=ism.

Ameri, A. (n.d.). *Risk management: The five pillars of information security*. Retrieved from http://cf.rims.org/Magazine/PrintTemplate.cfm?AID=2409.

Arrunadayy, K. (2017). *What's the 5 pillars of information security?*. Retrieved from https://www.quora.com/Whats-the-5-pillars-of-information-security.

Bayuk, J. (2009). *How to write an information security policy*. Retrieved from https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html.

Barman, S. (2016). *Information security governance and risk management.* Retrieved from https://www.simplilearn.com/cyber-security-interview-questions-and-answers-article.

Barnatt, C. (2017). *Computing security.* Retrieved from http://www.explainingcomputers.com/security.html.

Biscoe, C. (2017a). *7 steps to a successful ISO 27001 risk assessment*. Retrieved https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment/.

Biscoe, C. (2017b). *Top 10 risks to include in an information security risk assessment*. Retrieved https://www.vigilantsoftware.co.uk/blog/top-10-risks-to-include-in-an-information-security-risk-assessment/.

Bizcommunity. (2015). *More African countries exposed to mobile malware.* Retrieved from http://www.bizcommunity.com/Article/196/661/138771.html.

Blackstone, A. (2016). *Principles of sociological inquiry: Qualitative and quantitative methods, v. 1.0.* Retrieved from

http://catalog.flatworldknowledge.com/bookhub/reader/3585?e=blackstone_1.0-ch02_s03.

Borgatti, S. P. (1999). *Elements of research*. Retrieved from https://www.google.com.na/url?sa=t&rct=j&q=&esrc=s&source=web&cd=21&cad=rja&uact=8&ved=0ahUKEwi0sqb_hcPYAhUICsAKHeaTAowQFgigATAU&url=http%3A%2F%2Fwww.analytictech.com%2Fmb313%2Felements.htm&usg=AOvVaw3wBaWioTqoQHt5EEa66VD9.

Bowen, P., Hash. J., & Wilson, M. (2006). *Information security handbook: A guide for managers.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

Brikci, N., & Green, J. (2007). *A guide to using qualitative research methodology.* Retrieved from http://fieldresearch.msf.org/msf/bitstream/10144/84230/1/Qualitative%20research%20methodology.pdf.

BSI. (n.d.-a). *Central Bank of Nigeria to deliver the highest standards of Information Security.* Retrieved from https://www.bsigroup.com/LocalFiles/en-AE/Case%20Studies/ISO%2027001%20Case%20studies/ISO%2027001_Central_Bank_NigeriaCase%20Study%20LOWRES.pdf.

BSI. (n.d.-b). *Gulf Insurance Group K.S.C (GIG) increases their resilience to reassure clients and gain a competitive edge by implementing ISO 27001.* Retrieved from https://www.bsigroup.com/LocalFiles/en-AE/Case%20Studies/Gulf%20Insurance/Gulf%20Insurance%20Case%20Study.pdf.

BSI. (n.d.-c). *Nigeria Social Insurance Trust Fund (NSITF) is increasing its resilience with ISO 27001 Certification.* Retrieved from https://www.bsigroup.com/LocalFiles/en-AE/Case%20Studies/NSITF/NSITF%20HR%20Final.pdf.

BSI. (2008). *BSI-Standard 100-1: Information Security Management Systems (ISMS).* Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1.

BSI. (2009). *Standards - Implementing ISO/IEC 27001.* Retrieved from https://www.qualitydigest.com/inside/twitter-ed/implementing-isoiec-27001.html#.

BusinessDictionary. (2015). *Policy framework.* Retrieved from http://www.businessdictionary.com/definition/policy-framework.html

Charu, P. (2011). *Planning for and Implementing ISO 27001.* Retrieved from https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx.

Cisco. (2014). *Data leakage worldwide: Common risks and mistakes employees make.* Retrieved https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Collins. (2018a). *Definition of important.* Retrieved from https://www.collinsdictionary.com/dictionary/english/important.

Collins. (2018b). *Definition of 'relevant'.* Retrieved from https://www.collinsdictionary.com/dictionary/english/relevant.

Colorado State University. (2015). *Case studies: Definition and overview.* Retrieved from http://writing.colostate.edu/guides/page.cfm?pageid=1285&guideid=60.

CRAN. (n.d.). *About us*. Retrieved from http://www.cran.na/aboutus.html

Countrymeters. (2018). *Namibia population*. Retrieved from http://countrymeters.info/en/Namibia.

Creswell, J.W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). California: Sage Publication.

DCC. (2015). *Information security management: The ISO 27000 (ISO 27K) SERIES*. Retrieved from http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s.

Diego, P. (2018). *What is data security.* Retrieved from https://auth0.com/blog/what-is-data-security/.

Dudovskiy, J. (2017). *Research methodology.* Retrieved from https://research-methodology.net/research-methodology/research-approach/inductive-approach-2/.

Duke University. (2013). *Required elements of consent (from the Federal Regulations for Protecting Research Subjects): Basic Elements*. Retrieved from https://ors.duke.edu/researcher/informed-consent%20.

Dutton, J. (2017). *Three pillars of cyber security*. Retrieved from https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/.

eFortresses. (n.d.). *Readiness consulting - ISMS - ISO 27000 series: What is the ISO 27000 series?*. Retrieved from http://www.efortresses.com/services.htm.

Elky, S. (2006). *An introduction to information system risk management*. Retrieved https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.

Evaluation Research Team. (2008). *Data collection methods for program evaluation: Focus groups*. Retrieved from https://www.cdc.gov/healthyyouth/evaluation/pdf/brief13.pdf.

Evaluation Research Team. (2009). *Data collection methods for evaluation: Document review*. Retrieved from https://www.cdc.gov/healthyyouth/evaluation/pdf/brief18.pdf.

Fedco. (2015). *Continual improvement in ISO 27001 PDCA life cycle*. Retrieved from http://fedco.co.id/continual-improvement-in-iso-27001-pdca-life-cycle/.

Financial Times. (n.d.). *Definition of risk management.* Retrieved from http://lexicon.ft.com/Term?term=risk-management.

Ford, N. (2013). *People, processes and technology: the cyber security trinity*. Retrieved https://www.itgovernance.co.uk/blog/people-processes-and-technology-the-cyber-security-trinity/.

Frisken, J. (2015). *Leveraging COBIT to Implement Information Security.* Retrieved from http://www.isaca.org/COBIT/focus/Pages/leveraging-cobit-to-implement-information-security.aspx.

Gardner, M. (2017). *ISO 27001:2013 – Free gap analysis spreadsheet tool.* Retrieved from http://quality.eqms.co.uk/blog/free-iso-27001-gap-analysis-spreadsheet.

Gillies, A. (2011). *The TQM journal: Improving the quality of information security management systems with ISO27000*. Retrieved from https://www.emeraldinsight.com/doi/abs/10.1108/17542731111139455.

Gönderi, T. (2016). *Interactions in between ITIL, COBIT and ISO27001.* Retrieved from https://abdulkadirerkmen.wordpress.com/2016/03/04/interactions-in-between-itil-cobit-and-iso27001/.

Granneman, J. (2013). *IT security frameworks and standards: Choosing the right one.* Retrieved from http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one.

Green, R.H. (2018). *Namibia.* Retrieved from https://www.britannica.com/place/Namibia.

Gunnels, A. (2018). *What is computer security? - Definition & Basics.* Retrieved from https://study.com/academy/lesson/what-is-computer-security-definition-basics.html.

Halkyn Security. (2013). *ISO27001 compliance checklist available for download.* Retrieved from https://www.halkynconsulting.co.uk/a/2013/10/iso27001-compliance-checklist/.

Haseeb, A.A. (2016). *Why ISO/IEC 27001 Information security certification is compulsory for companies*. Retrieved from http://www.haseebayazi.com/2016/02/why-isoiec-27001-information-security.html.

Hau, D. (2003). *Unauthorised access - Threats, risk and control*. Retrieved https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/.

Heriot-Watt University. (2013). *Information security policy framework.* Retrieved from https://www.hw.ac.uk/documents/information-security-policy-framework.pdf.

Hevner, A.R. (2007). *A three cycle view of design science research.* Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1017&context=sjis.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). *Design science in information systems research. MIS Quartely*, 75-105. Retrieved from https://pdfs.semanticscholar.org/fa72/91f2073cb6fdbdd7c2213bf6d776d0ab411c.pdf.

International Organisation for Standardization. (2018). *Information technology - Security techniques - Information security management systems - Overview and vocabulary (*ISO/IEC 27000:2018(en)). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.

International Organisation for Standardization/International Electrotechnical Commission. (2013a). *Information technology - Security techniques - Code of practice for information security controls* (ISO/IEC 27002:2013(E)). Geneva, Switzerland: ISO/IEC.

International Organisation for Standardization/International Electrotechnical Commission. (2013b). *Information technology - Security techniques - Information security management systems - Requirements* (ISO/IEC 27001:2013(E)). Geneva, Switzerland: ISO/IEC.

Internet World Stats. (2011). *Usage and population statistics: Africa.* Retrieved from https://www.internetworldstats.com/af/na.htm.

Irwin, L. (2017). *How to implement an ISMS.* Retrieved from https://www.itgovernance.co.uk/blog/how-to-implement-an-isms/.

ISACA. (2009). *An introduction to the business model for information security.* Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf.

ISO. (n.d.-a). ISO/IEC 27001: *Information security management*. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

ISO. (n.d.-b). *ISO/IEC 27004:2016*. Retrieved from https://www.iso.org/standard/64120.html.

ISO. (n.d.-c). Namibia (NSI): *Membership: Member body*. Retrieved from http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1569.

ISO. (2016). *ISO/IEC 27000:2016.* Retrieved from https://www.iso.org/standard/66435.html.

ISO. (2014). *ISO/IEC 27000:2014*. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411.

ISO/IEC. (2016). *International Standard ISO/IEC 27004:2016*. Retrieved from https://webstore.ansi.org/Previews/PREVIEW_ISO+IEC+27004-2016.pdf.

ItGovernance. (2015). *ISO27000 family of standards: The ISO/IEC 27000 family of information security standards.* Retrieved from http://www.itgovernance.co.uk/iso27000-family.aspx#.VSuId_nF_y4.

ItGovernance. (2017*). ISO27003 (ISO 27003) ISMS implementation guidance*. Retrieved from https://www.itgovernance.co.uk/shop/product/iso27003-iso-27003-isms-implementation-guidance.

IT News Africa. (2016). *Namibia still a top target for cybercriminals*. Retrieved from http://www.itnewsafrica.com/2016/01/namibia-still-a-top-target-for-cybercriminals/.

ITU. (2017). *Readiness assessment report to establish a national CIRT for Namibia.* Retrieved from

Janes, P. (2012). *People, process, and technologies impact on information data loss*. Retrieved https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032.

Johannesson, P. & Perjons, E. (2014). *An introduction to design science.* Retrieved from http://common.books24x7.com/toc.aspx?bookid=77009.

Johnson, A., Katzke, S., Rogers, G., Ross, R., Stoneburner, G., & Swanson, M. (2006). *Information Security*. Retrieved from https://www.govinfo.gov/content/pkg/GOVPUB-C13-23ee274448482b01bbc325f6ce470e30/pdf/GOVPUB-C13-23ee274448482b01bbc325f6ce470e30.pdf.

Kadam, A. (2003). *Implementation methodology for information security management system (to comply with BS 7799 Requirements).* Retrieved from https://cyber-defense.sans.org/resources/papers/gsec/implementation-methodology-information-security-management-system-to-comply-bs-7799-requi-104600.

Kaspersky. (2015). *Kaspersky security bulletin 2015*. Retrieved from https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Kathindi, A. (2015). *WACS capacity to increase to 45%.* Retrieved from https://www.thevillager.com.na/articles/9165/WACS-capacity-to-increase-to-45-/.

Kearns, G.S. (2016). *Countering mobile device threats: A mobile device security model.* Retrieved from http://web.nacva.com/JFIA/Issues/JFIA-2016-4.pdf.

Kelechava, B. (2017). *Information security management system (ISO/IEC 27000 Series)*. Retrieved from https://blog.ansi.org/2017/01/information-security-management-system-isoiec/#gref.

Kosutic, D. (n.d.-a). *ISO 27001:2013 foundations course* [Video file]. Retrieved from https://training.advisera.com/start-course/.

Kosutic, D. (n.d.-b). *ISO 27001 gap analysis vs. risk assessment*. Retrieved from http://advisera.com/27001academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment/.

Kosutic, D. (2014). *Which one to go with – Cybersecurity framework or ISO 27001?*. Retrieved from https://advisera.com/27001academy/blog/2014/02/24/which-one-to-go-with-cybersecurity-framework-or-iso-27001/.

Kosutic, D. (2018). *ISO 27001 implementation checklist.* Retrieved from https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/.

Kiilu, P.K., & Nzuki, D.M. (2015). *Factors affecting adoption of information security management systems: A theoretical review CPA.* Retrieved from https://www.ijsr.net/archive/v5i12/ART20163327.pdf.

Kissel, R. (2013). *Glossary of key information security terms.* Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Kostadinov, D. (2014). *Key elements of an information security policy*. Retrieved from http://resources.infosecinstitute.com/key-elements-information-security-policy/#gref

Lachapelle, E., & Mustafë, B. (2016). *ISO/IEC 27002:2013*. Retrieved from http://zih.hr/sites/zih.hr/files/cr-collections/3/iso27002.pdf.

Lapadat, J.C. (2010). *Encyclopedia of case study research.* Retrieved from http://sk.sagepub.com/reference/download/casestudy/n342.pdf.

Lehtinen, R., Russell, D., & Gangemi, G.T. (2006). *Network security basics*. USA: O'Reilly.

Lindros, K. (2017). *What is IT governance? A formal way to align IT & business strategy.* Retrieved from https://www.cio.com/article/2438931/governance/governanceit-governance-definition-and-solutions.html.

Lord, N. (2017). *What is NIST SP 800-53? Definition and tips for NIST SP 800-53 compliance.* Retrieved from https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance.

Lourens, N. (2018). *Namibia connected.* Retrieved from https://www.namhost.com/blog/namibia/definitive-guide-internet-namibia.

March, S.T., & Smith, G.F. (1995). *Design and natural science research on information technology.* Retrieved from https://pdfs.semanticscholar.org/d93f/fe572b15a163e2ec1336a4e507b0b7a766f0.pdf.

Maree, J.G. (2007). *First steps in research.* Pretoria, South Africa: Van Schaik Publishers.

McLaughlin, E. (2016). *Definition: data collection.* Retrieved from http://searchcio.techtarget.com/definition/data-collection.

MICT. (n.d.). About. Retrieved from https://www.facebook.com/pg/mictnamibia/about/?ref=page_internal

Mills, C.D. (2016). *Security controls.* Retrieved from https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Security_Controls.

Minister of Information Communications and Technology. (n.d.). *Bill*. Retrieved from http://www.mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25.

Mora, M. (2010). *Quantitative Vs. qualitative research: When to use which.* Retrieved from http://www.surveygizmo.com/survey-blog/quantitative-qualitative-research/.

Mydesktops. (n.d.). *Types of controls.* Retrieved from https://infosecprimer.wordpress.com/2012/11/03/types-of-controls/.

Newitz, A. (2015). *9 Facts about computer security that experts wish you knew.* Retrieved from https://gizmodo.com/9-facts-about-computer-security-that-experts-wish-you-k-1686817774.

Noticebored. (2017a). *ISO/IEC 27003*. Retrieved from http://www.iso27001security.com/html/27003.html.

Noticebored. (2017b). *ISO27k timeline*. Retrieved from http://www.iso27001security.com/html/timeline.html.

Oates, B.J. (2012). *Researching information systems and computing.* Los Angeles: Sage Publishers

Office of the Minister of State for Administrative Reform. (n.d). *Lebanese national cyber security policy guidelines*. Retrieved from http://www.omsar.gov.lb/CyberSecurityPolicy/Lebanese%20National%20Cyber%20Security%20Policy%20Guidelines%20v1.7.pdf.

Office of the Prime Minister.(n.d.). *Task-enforcement.* Retrieved from http://www.opm.gov.na/task-enforcement.

Olivier, F. (2017). *Cybercrime in Namibia*. Retrieved from https://www.namibian.com.na/165301/archive-read/Cybercrime-in-Namibia.

Olsen, B. (2014). *Protect your data: Focus on cyber security's 3 pillars.* Retrieved from https://www.compasscyber.com/blog/protect-data-focus-cyber-securitys-3-pillars/.

Pandey, S.C. & Patnaik, S. (2014). Establishing reliability and validity in qualitative inquiry: A critical examination. *Jharkhand Journal of Development and Management Studies XISS*, *12*(1), 5743 – 5753.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 47-77.

Peltier, T.R. (2010). *Information security risk analysis.* (3rd ed.). Retrieved from http://common.books24x7.com/toc.aspx?bookid=36951.

Pesante, L. (2008). *Introduction to information security*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf.

Queensland Government. (2017). *Implementing an ISMS.* Retrieved from https://www.qgcio.qld.gov.au/__data/assets/pdf_file/0024/11697/Implementing-an-ISMS-Participant-Guide-V1.1.pdf.

Quizlet. (n.d.). *CISSP information security and risk management.* Retrieved from https://quizlet.com/8687743/cissp-information-security-and-risk-management-set-2-flash-cards/.

Regoniel, P. (2010). *What is the difference between the theoretical and the conceptual framework?* Retrieved from https://college-college-life.knoji.com/what-is-the-difference-between-the-theoretical-framework-and-the-conceptual-framework/.

Rose, M. (2013). *COBIT.* Retrieved from http://searchsecurity.techtarget.com/definition/COBIT.

Rose, M. (2014). *ITIL: Information technology infrastructure library.* Retrieved from http://searchdatacenter.techtarget.com/definition/ITIL.

Rouse, M. (2006). *Definition ISP -Internet service provider*. Retrieved from http://searchwindevelopment.techtarget.com/definition/ISP.

Rouse, M. (2009). *ISO 27001- What is ISO 27001?.* Retrieved from http://whatis.techtarget.com/definition/ISO-27001.

Rouse, M. (2011). *Information security management system (ISMS).* Retrieved from https://whatis.techtarget.com/definition/information-security-management-system-ISMS.

Rouse, M. (2013). *Longitudinal study*. Retrieved from http://whatis.techtarget.com/definition/longitudinal-study.

Rouse, M. (2015). *Implementation.* Retrieved from https://searchcrm.techtarget.com/definition/implementation

SANS. (2018). *Network security resources.* Retrieved from https://www.sans.org/network-security/.

SANS Institute. (2007). *Information security policy – A development guide for large and small companies.* Retrieved from https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331.

Saunders, M., Philip, L., & Thornhill, A. (2009) *Research methods for business students (5th ed.).* Retrieved from http://www.dphu.org/uploads/attachements/books/books_5236_0.pdf.

Sharma, R. (2012). *What is the difference between risk identification and risk assessment?.* Retrieved from https://www.brighthubpm.com/risk-management/89885-what-is-the-difference-between-risk-identification-and-risk-assessment/.

Shaw, R. (2012). *Conducting an information security gap analysis.* Retrieved from https://images.template.net/wp-content/uploads/2016/01/04125735/Information-Security-Gap-Analysis-PDF-Format-Download.pdf.

Sehlhorst, S. (2007). *What are use case scenarios?* Retrieved from http://tynerblain.com/blog/2007/04/10/what-are-use-case-scenarios/.

Sell, C. (2015). *How to conduct an information security gap analysis.* Retrieved from https://www.cio.com/article/2876708/security0/how-to-conduct-an-information-security-gap-analysis.html.

Shojaie , B., Federrath, H., & Saberi, I. (2015). *The effects of cultural dimensions on the development of an ISMS based on the ISO 27001*. *IEEE*. Retrieved from https://ieeexplore.ieee.org/document/7299909/.

Shuttleworth, M. (2008). *Case study research design.* Retrieved from https://explorable.com/case-study-research-design.

Shuttleworth, M. (2009). *What is a literature review?*. Retrieved from https://explorable.com/what-is-a-literature-review.

Singh, A. (2017). *Three pillars of a successful security strategy*. Retrieved from https://solutionsreview.com/security-information-event-management/three-pillars-of-a-successful-security-strategy/.

Smith, J. M. (2018). *Serious flaws in cybersecurity bill.* Retrieved from https://www.namibiansun.com/news/serious-flaws-in-cybersecurity-bill2018-02-12/?.

Song, K. (2017). *Exploring the factors influencing the adoption of ISMS standards or frameworks.* Retrieved from https://scss.tcd.ie/publications/theses/diss/2017/TCD-SCSS-DISSERTATION-2017-056.pdf.

Spruit, M.E.M., & Samwel, P.H. (n.d.). *Risk analysis on Internet connection.* Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.1316&rep=rep1&type=pdf.

Sudeshna, D., & Shruti, D. (2016). *Importance of research approach in a research.* Retrieved from https://www.projectguru.in/publications/selecting-research-approach-business-studies/.

Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information security management system standards: A comparative study of the Big Five. *International Journal of Electrical & Computer Sciences*, *11*(5). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.8070&rep=rep1&type=pdf.

Techopedia. (2018a). *Information security management system (ISMS).* Retrieved from https://www.techopedia.com/definition/16515/information-security-management-system-isms.

Techopedia. (2018b). *NIST 800-53*. Retrieved from https://www.techopedia.com/definition/28830/nist-800-53.

THEINFOSECGURU. (2014). *Information security domains: more than 10 possible?* Retrieved from https://theinfosecguru.wordpress.com/2014/05/16/infosec-domains/.

The Agnosticator. (2013). *A comparison of COBIT, ITIL, ISO 27002 and NIST.* Retrieved from http://agnosticationater.blogspot.com/2013/12/a-comparison-of-cobit-itil-iso-27002.html.

The Government of the Hong Kong Special Administrative Region. (2018). *IT Security standards and best practices.* Retrieved from https://www.infosec.gov.hk/english/technical/standards.html.

The Writing Center. (2018). *Literature reviews*. Retrieved from https://writingcenter.unc.edu/tips-and-tools/literature-reviews/.

Tipton, H.F., & Krause, M. (2007). *Information security management handbook* (6th ed). volume 1. [Books24x7 version] Retrieved from http://common.books24x7.com/toc.aspx?bookid=26438.

Tjirare, D.J., & Bhunu Shava, F. (2017). *A gap analysis of the ISO/IEC 27000 standard implementation in Namibia.* Paper presented at IST-Africa Week Conference (IST-Africa), 2017, Windhoek. doi:10.23919/ISTAFRICA.2017.8102376.

UK Essays. (2015). *Research methodology, different types of philosophical.* Retrieved from https://www.ukessays.com/essays/psychology/research-methology-is-a-study-which-raises-types-of-philosophical-psychology-essay.php.

United State Naval Academy. (n.d.). *Pillars of cyber security*. Retrieved from https://www.usna.edu/CyberDept/sy110/lec/pillarsCybSec/lec.html.

Uudhila, J.M. (2016). *Cyber security risk management and threat control model (CSRM-TCM): A study carried out to enhance the protection of information in the Namibian public service.* Retrieved from https://repository.unam.edu.na/bitstream/handle/11070/1688/Uudhila_2016.pdf?sequence=1.

Vaishnavi, V., Kuechler, W., & Petter, S. (Eds.). (2017). *Design science research in information systems.* Retrieved from http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf.

Vaishnavi, V., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*, (2nd ed.). Retrieved from http://common.books24x7.com/toc.aspx?bookid=74154.

Vinz, S. (2017). *The theoretical framework of a thesis: what and how?* Retrieved from https://www.scribbr.com/thesis/the-theoretical-framework-of-a-thesis-what-and-how/.

Vogel, V. (2014). *Information security governance.* Retrieved from https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Governance.

Warren, K.V. (2010). *Security controls in service management.* Retrieved from https://www.sans.org/reading-room/whitepapers/iso17799/security-controls-service-management-33558.

Webopedia. (2015). *Security policy.* Retrieved from http://www.webopedia.com/TERM/S/security_policy.html.

Wikipedia. (2017). *Information security management.* Retrieved from https://en.wikipedia.org/wiki/Information_security_management

Whitman, M.E., & Mattord, H.J. (2012). *Principles of information security: Introduction to information security* (4th ed.). Retrieved from https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf.

Wyse, S.E. (2011). *What's the difference between qualitative and quantitative research?* Retrieved from https://www.snapsurveys.com/blog/qualitative-vs-quantitative-research/.

Yau, H.K. (2014). *Information security controls*. Retrieved from https://www.omicsonline.org/open-access/information-security-controls-2168-9695.1000e118.php?aid=23716.

Yin, R. K. (2009). *Case study research: Design and ethods* (Vol. 5). California: Sage Publications.

Yin, R. K. (2011). *Qualitative research from start to finish*. New York,NY: The Guilford Press.

APPENDIX A: REQUEST FOR PERMISSION TO CONDUCT RESEARCH

My name is Diana J. Tjirare and I am an Information Technology student at the Namibia University of Science and Technology. I'm conducting a research for the MASTER OF COMPUTER SCIENCE which involves implementing an ISO/IEC 27000 framework for security standards in Namibia. This project will be conducted under the supervision of Mrs. Fungai Bhunu Shava.

Implementing an ISO27000 framework for security standards will provide the following benefits to organisations:

- ✓ Information security issues, and how to mitigate associated risks, will be identified, managed, monitored and improved in a planned manner
- ✓ The correct information security management processes and procedures will be defined, documented and put in to practice
- ✓ Demonstration of organisational commitment to information security, will ensure adequate allocation of resources, identification of roles and responsibilities and appropriate training
- ✓ Data will be protected against unauthorised access and it will be available to authorised user when they require it, demonstrating the organisation security posture.
- ✓ An organisation's profile will improve and business opportunities will increase if the continuity of an organisation's business is effectively managed
- ✓ Intellectual property rights can be protected
- ✓ An organisation confirming independently to the standard compliance can guarantee that it has not been inconsiderate in regards to suitable laws on the protection of individual data

I am hereby seeking your consent to contact a survey at your organisation. The survey will be an online based questionnaire, were by a link will be provided to complete the questionnaire. An interview will be conducted as a follow up, to clarify any issue that might be omitted from the interview. Participation is voluntary.

Information collected will be kept strictly confidential and will be used for the purpose of the research only. If you require any further information, please do not hesitate to contact me on 0855601000 or dkanikin@gmail.com. Thank you for your time and consideration in the matter.

Researcher: Diana J. Tjirare IT department staff:

Signature: …….. Signature: ……

APPENDIX B: Semi-structured Interview Questions

1. Is the ISO 27000 family of standards implemented in your organisation?

2. Does your organisation have documented Information Technology security standard policies?

3. What are the factors affecting the adoption of ISO 27000 family of standards?

4. Who governs security policies?

5. Do you have any plans of implementing the ISO 27000 family of standards as a security solution to the current challenges?

APPENDIX C: Conference Paper

IST-Africa
IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-56-4

A Gap Analysis of the ISO/IEC 27000 Standard Implementation in Namibia

Diana Jogbeth TJIRARE[1], Fungai BHUNU SHAVA[2]
Namibia University of Science and Technology, Address, Windhoek, 9000, Namibia
[1]*Tel: +264 811492639, Fax: + 264 088624060, Email: dkanikin@gmail.com*
[2]*Tel: +264 61 2072510, Fax: + 264 61 2079510, Email: fbshava@nust.na*

Abstract: To ensure that the information asset is protected and available to organisations, information security needs to be governed by security standards. The ISO/IEC 27000 family of standards is one such standard; it keeps information assets secure and provides an information security management best practises framework. Despite its importance, the usage and adoption of the ISO/IEC 27000 standards is missing in Namibian organisations. An exploratory pilot survey conducted in 2015 with the key stakeholders namely the Communications Regulatory Authority, Internet Service Providers and government departments revealed that these standards are not being implemented at all. Based on literature review and the preliminary surveys, this paper presents the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia. The study will focus on the implementation extent for ISO 27000, 27001, 27002, 27003 and 27004 as these are the critical standards to the security posture of any organisation. A qualitative case study research approach with security critical organisations in Namibia was used for this study. Surveys and interviews were used to collect data from purposefully identified key stakeholders. The stakeholders offered rich information about the phenomenon under study. The survey results were used to evaluate the extent of implementation and the factors contributing to the poor implementation. A theoretical framework was derived from the findings and is thus presented in this paper. The factors making up the theoretical framework will be used as a basis in designing a policy framework for the adoption of security standards by organisations in Namibia to secure its critical assets, manage risks more effectively, improve and maintain customer confidence, demonstrate conformance to international best practice, avoid brand damage and change its information security posture as the technology is evolving.

Keywords: Security policy, Policy framework, ISO 27000, Information security, Information Security Policies

1. Introduction

As Namibia is developing, the increase in information technology usage is also noticed, as attested by the 100% growth in internet usage in 2015 compared to the year 2000 [1]. To ensure that the information asset is protected and beneficial to organizations in Namibia, information access needs to be governed. One of the standards used for Information security governance is the ISO/IEC (International Organization for Standardization) 27000 family of standards. The ISO/IEC 27000 family of standards provides a globally recognised information security management framework best-practice [2]. According to [3] ISO 27000 family of standards provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS).

The aim of the study was to investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia. The study focused on the implementation extent for ISO 27000, 27001, 27002, 27003 and 27004 as these are the

Copyright © 2017 The authors

critical standards to the security posture of any organisation to mitigate information security risks and as such the security of the nation. This paper presents the findings of a preliminary study conducted in Namibia to investigate the factors influencing the adoption of ISO27000 standards. It is aimed at raising awareness among the stakeholders on the state of affairs and how the landscape can be influenced for a secure Namibia.

This section introduced the paper by stating the overview and purpose of the paper. The next sections will discuss the background, objectives, methodology, case study, theoretical framework and business benefits relevant to this paper. A conclusion section is also included to summarise the paper.

1.1 Background

To ensure a suitable level of security is maintained, resources are correctly used, and the security practices are adopted [4] good information security governance should be implemented in organisations. Furthermore [5] states that the aim of information security governance is to make sure that organisations are effectively implementing appropriate information security controls to support their mission in a cost-effective manner, while managing evolving information security risks. The process of establishing and maintaining a framework, supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives all in an effort to manage risk is called Information security governance [5]. This is usually achieved by using information governance standards.

Information governance standards are listed below:

COBIT (Control Objectives for Information and Related Technology) - is a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices [6].

ITIL (Information Technology Infrastructure Library) - framework is designed to standardize the selection, planning, delivery and support of IT services to a business to improve efficiency and achieve predictable service levels [7].

NIST 800-53 (National Institute of Standards and Technology) - provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate contributing to systems that are more resilient in the face of cyber-attacks and other threats [8].

ISO 27000 - provides a very broad information security framework that can be applied to all types and sizes of organizations [9].

The research project will focus on ISO 27000 family standards.

1.2 ISO 27000 family of Standards

ISO 27000 family of standard was originally published as British Standard 7799 in 1995 and then later as ISO 17799 [10]. While there are several standards in the ISO 27000 family of standards this project will focus on the five standards listed below with their purpose: [11]

ISO/IEC 27000 - ISMS overview and vocabulary
ISO/IEC 27001 - ISMS requirements
ISO/IEC 27002 - Code of practice for information security controls
ISO/IEC 27003 - ISMS implementation guidance
ISO/IEC 27004 - Information security management measurement

The ISO/IEC 27000 is a collection of standards that specify the complete implementation of an Information Security Management Systems (ISMS) when used together [12].

Furthermore [12] states that policies, procedures, human and machine resources which are part of ISMS should maintain the CIA Triad (Confidentiality, Integrity and Availability) across an organisation.

The ISO 27000 series provides recommendations for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System [13].

According to [12] implementing the ISO 27000 family of standards can bring the benefits listed below to an organisation:

- Information security issues, and how to mitigate associated risks, will be identified, managed, monitored and improved in a planned manner
- The correct information security management processes and procedures will be defined, documented and put into practice
- Demonstration of organisational commitment to information security, will ensure adequate allocation of resources, identification of roles and responsibilities and appropriate training
- Data will be protected against unauthorised access and it will be available to authorised user when they require it, demonstrating the organisation security posture.
- An organisation's profile will improve and business opportunities will increase if the continuity of an organisation's business is effectively managed
- Intellectual property rights can be protected
- An organisation confirming independently to the standard compliance can guarantee that it has not been inconsiderate in regard to suitable laws on the protection of individual data

It is evident that when organisations and nations adopt and implement these standards, their security postures will be greatly improved. In the next section the case site is described in detail.

2. Objectives

The objective of the study was to investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia, and design a theoretical framework that will inform the design of a policy framework to enable the implementation of security best practice in Namibia.

3. Methodology

A qualitative case study research approach with security critical organisations in Namibia was used for this study. Qualitative research generates words, rather than numbers, as data for analysis [14]. Qualitative research was used in this case to help us understand the phenomenon, this helped us to define the problem and develop an approach to the problem [15]. Case study refers to gathering and producing detailed information about individuals or collective group of people regularly including the actions of the individuals [16].

Survey and interviews were used to collect data from the identified stakeholders namely the Communications Regulatory Authority, Internet Service Providers and government departments. The stakeholders were purposefully selected as they offer rich information about the phenomenon under study. The survey results and literature review were used for gap analysis to identify and validate the implementation extent of the ISO 27000 security standards. A theoretical framework was derived from the findings and is thus presented in this paper. According to [17] a theoretical framework provides a general representation of relationships between things in a given phenomenon. Additionally [17] a theoretical framework dwells on time tested theories that represent the findings of different

investigations on how phenomena occur. The steps below from [18] were used to develop the theoretical framework:

- Select key concepts listed below
- ✓ Sample problem statement and research questions
- ✓ Problem
- ✓ Objective
- ✓ Research question
- Define and evaluate relevant concepts, theories, and models
- Consider adding other elements to your theoretical framework

To ensure that the different selected stakeholders are aware of ethical issues for this research project a consent form was prepared and distributed to the stakeholders.

This research paper is limited to a case analysis of identified stakeholders. Several literatures studied on the standards usage elsewhere to benchmark the policy framework implementation specific to Namibia were consulted.

4. Case Study

Namibia is a nation with a population of 2,5 million [19] and depends on ICTs to run its businesses and drive its economy. To manage the ICTs and ensure proper implementation the following structure is in place:

The Office of the Prime Minister (OPM) is responsible for strategic plan, co-ordination of cabinet matters and projects/programs [20], the Ministry of ICT is responsible for the development and promotion of ICT growth, and provide effective information service, promote constructive dialogue towards socio-economic development and democracy[21], Communication Regulatory Authority of Namibia (CRAN) was enacted with a mandate to regulate the operation of telecommunication services and networks, broadcasting services, postal services and the use and allocation of radio spectrum [22], on the other hand Internet Service Providers (ISPs) are responsible for providing individuals and other companies access to the Internet and other related services [23], the Namibia Institute of Standards(NIS) is responsible for promotion of standardization and quality assurance in the industry, commerce and the public sector in Namibia [24], these critical organisations are responsible for ensuring secure access of authorised content to citizens.

5. Theoretical Framework Design

A theoretical framework for this study was developed using the steps below from [18]:

5.1 Select Key Concepts Listed Below

- Problem statement - The ISO/IEC 27000 family of standards provides a globally recognised information security management framework best-practice [2]. Namibia was the second most attacked country in November 2015 after being the most targeted by cybercriminals during December 2015 [26]. To what extent is Namibia implementing these best practices to ensure secure cyber experiences for her citizens?
- Problem – to what extent is Namibia implementing best practice standards to change its rating as one of the most vulnerable country to cyber criminals?
- Objective - The objective of the study was to investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia, and designs a theoretical framework that will inform the stakeholders on the extent of the implementation of security best practice in Namibia.
- Research question - What is the extent of the ISO/IEC 27000 implementation framework adoption in Namibia?

5.2 *Define and Evaluate Relevant Concepts, Theories and Models*

According to [27] security best practices are missing in the Namibian Public Service and hence IT personnel are finding it difficult to manage the security of different Information Systems.

In the paper written by [25] the "Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned" the following are obstacles when implementing ISO 27001, identifying organization's assets, weak team experience, resistant to change, unclear understanding of standard, top management involvement and Saudi Arabia's Culture

The adoption of Information Security standards requires discipline, proper documentation, and adequate budget, enforcement of policies and procedures and deployment of the right personnel [28].

The implementation and adoption of the ISO 27000 standard in Namibia might also be caused by the factors mentioned above. To again further understanding, a gap analysis was conducted. The process of investigating the extent to which the ISO/IEC 27000 standard is implemented is described as gap analysis [29]. Gap analysis is reviewing each section of ISO 27001 document and determining if that requirement is already implemented in an organisation [29]. The scale below was identified from literature review to determine the extent of ISO 27000 family of standard implementation [29]:

- 0 – requirement not implemented nor planned
- 1 – requirement is planned but not implemented
- 2 – requirement is implemented only partially, so that full effects cannot be expected
- 3 – requirement is implemented, but measurement, review and improvement are not performed
- 4 – requirement is implemented and measurement, review and improvement are performed regularly

5.3 *Consider Adding Other Elements to Your Theoretical Framework*

The interviews and surveys with the regulatory board (CRAN), ISPs and government departments revealed that the standard is not implemented. Namibia is a member of ISO and however after preliminary interviews with stakeholders, other factors peculiar to Namibia were identified and will be added to the framework.

5.4 *Case Study Results*

Using the gap analysis scale, it was established through the exploratory pilot gap analysis survey conducted in 2015 with CRAN, ISPs, NIS and government departments it was established that Namibia is at the 0 – requirement not implemented nor planned level.

The implications of not implementing the standards are confidentiality breaches, unauthorized alteration of critical information, data leakage and a vulnerable nation. Namibia was the second most attacked country in November 2015 after being the most targeted by cybercriminals during December 2015[26].

From literature review factors affecting the adoption of the standards were identified as:

Identifying organization's assets; weak team experience, deployment of the wrong personnel; resistance to change; unclear understanding of standards; lack of top management involvement; culture; lack of discipline; improper documentation; inadequate budget; poor enforcement of policies and procedures [25] [28]. The survey focused on validating the weak team experience, deployment of the wrong personnel, improper documentation and poor enforcement of policies and procedures as this was considered key in establishing the baseline.

Based on literature review findings, the questions below were used during the pilot semi structured gap analysis survey to investigate the baseline for Namibia:

- Is the ISO 27000 family of standards implemented in your organisation?
- Does your organisation have documented Information Technology security standard policies?
- What are the factors affecting the adoption of ISO 27000 family of standards?
- Who governs security policies?
- Do you have any plans of implementing the ISO 27000 family of standards as a security solution to current challenges

The case study findings showed that the ISO 27000 family of standard is not used or implemented in Namibia. When asked if the ISO 27000 family of standards is implemented in their organisation, one participant said "The Cyber security bill is before parliament currently and the standard is not used or implemented in Namibia". The participant further stated that currently no one is certified for ISO 27001 standard in Namibia. NIS and OPM are responsible for security policy governance and the stakeholders have documented security policy, however they are not properly documented.

From the interviews the responses were in the following categories/themes

Security landscape	Factors affecting the adoption/implementation of ISO 27000	Mitigating strategy	Benefit of implementing ISO 27000 Standards
To gauge the security landscape. The question "Is the ISO 27000 family of standards implemented in your organisation?" was used and responses showed: Implementation Extent 0 – standards not implemented nor planned. In response to "Who governs security policies?", the stakeholders stated that NIS and OPM are responsible for security policy governance	In response to "What are the factors affecting the adoption of ISO 27000 family of standards?" Weak team experience or deployment of the wrong personnel was noted, the responses said "employees are not trained and are not certified in ISO 27001". In response to question two "• Does your organisation have documented Information Technology security standard policies?" the respondents noted that they have Improperly documented polices as well as poor enforcement of policies and procedures	When asked do you have any plans to implementing the ISO 27000 family of standards as a security solution to the current challenges? The stakeholders stated "Yes, The Cyber security bill is before parliament and ISO 27000 family of standards is part of this bill".	When asked about the cost benefit of ISO27000 implementation, the following were identified: 1. Protect crucial resources 2. Manage risks more efficiently 3. Improve and maintain customer confidence 4. Shows that they are adapting to international best practice 5. Avoid brand damage and change its information security posture alongside technological developments.

Table1: Summary of survey response and, the benefit and mitigating strategy of ISO 27000

After collecting primary data from the participants, the Gap Analysis was applied to determine the current posture of Namibia. Based on the survey and literature review

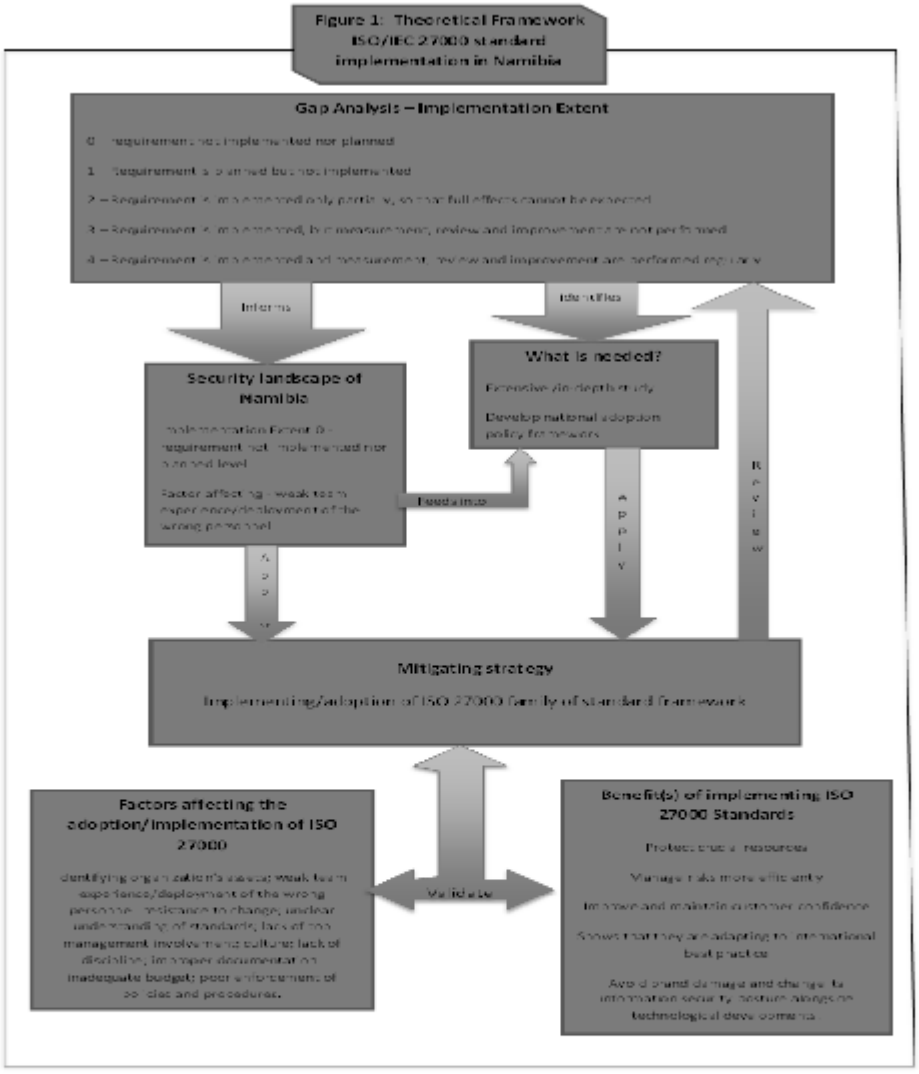
Namibia is at the extent 0 – standards not implemented nor planned however there is a consideration when the cyber security bill has gone through parliament. This shows that the nation is still at the baseline in terms of adopting the ISO 27000 family standard.

From the literature and survey, the key components to the assessment of the extent of adoption/implementation were identified as:

1. Security landscape
2. Factors affecting the adoption and implementation
3. Mitigating strategy
4. Cost benefit analysis
5. Gap analysis

These components were used in designing the framework. The relationships are shown in the framework.

The theoretical framework below shows the security of Namibia, possible mitigating strategies, the benefit of implementing the ISO/IEC 27000 standard, gap analysis scale, factors affecting the implementation and what still needs to be done to improve the security. When there is a clear understanding of the security posture of an organization, mitigation strategies can be evaluated and the best selected for adoption. However, before adopting a strategy the benefits need to be well understood, these will inform gap analysis and the establishment of factors that are critical to the success. Once this is clear steps can be listed which need to be effected to improve the posture. The framework presented in figure 1 is entirely based on the case study findings and is informed by the literature review. Framework evaluation will be conducted in future endeavours, as part of a larger study.



6. Business Benefits

Organisations in Namibia will gain the benefits listed below if they implement/adopt the ISO 27000 family of standard framework:

- Information security issues, and how to mitigate associated risks, will be identified, managed, monitored and improved in a planned manner
- The correct information security management processes and procedures will be defined, documented and put in to practice
- Demonstration of organisational commitment to information security, will ensure adequate allocation of resources, identification of roles and responsibilities and appropriate training

- Data will be protected against unauthorised access and it will be available to authorised user when they require it, demonstrating the organisation security posture.
- An organisation's profile will improve and business opportunities will increase if the continuity of an organisation's business is effectively managed
- Intellectual property rights can be protected
- An organisation confirming independently to the standard compliance can guarantee that it has not been inconsiderate in regard to suitable laws on the protection of individual data

7. Conclusions

The study intended to investigate the extent to which the ISO/IEC 27000 implementation framework is adopted in Namibia and it was revealed that the usage and adoption of the ISO/IEC 27000 standards is missing in Namibian organisations. Since Namibia is rated as one of the most vulnerable country to cyber criminals it definitely needs to implement these best practices to ensure secure cyber experiences.

A theoretical framework of the gap analysis on ISO/IEC27000 framework adoption was presented. The theoretical framework will serve as the basis for the development of an adoption policy framework for Namibia. A national adoption policy framework to ensure that all organisations in Namibia use information security best practices to mitigate information security risks should be designed. We recommend that an in-depth study is done and an information security framework is designed and regularly reviewed for any gap that might arise, to assist with the adoption and implementation of the standard.

References

[1] Internet World Stats. (2015). Usage and population statistics: Africa. Retrieved from http://www.internetworldstats.com/africa.htm#na

[2] itGovernance. (2015). ISO27000 family of standards: The ISO/IEC 27000 family of information security standards. Retrieved from http://www.itgovernance.co.uk/iso27000-family.aspx#.VSuId_nF_y4

[3] eFortresses. (n.d.). Readiness consulting - ISMS - ISO 27000 series: What is the ISO 27000 series?. Retrieved from http://www.efortresses.com/services.htm

[4] The Government of the Hong Kong Special Administrative Region. (2008). An overview of information security standards. Retrieved from http://www.infosec.gov.hk/english/technical/files/overview.pdf

[5] Bowen, P., Hash, J., & Wilson,M. (2006). Information Security Handbook: A Guide for Managers. Retrieved from http://www.mobileworkexchange.com/uploads/3000/2727-NIST_Information_Security_Handbook.pdf

[6] Rose, M. (2013). COBIT. Retrieved from http://searchsecurity.techtarget.com/definition/COBIT

[7] Rose, M. (2014). ITIL: Information technology infrastructure library. Retrieved from http://searchdatacenter.techtarget.com/definition/ITIL

[8] NIST. (2013). Security and privacy controls for federal information systems and organizations. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[9] Granneman, J. (2013). IT security frameworks and standards: Choosing the right one. Retrieved from http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

[10] Vanderburg, E. (n.d). Information security compliance: ISO 27000.I Retrieved from http://jurinnov.com/iso-27000-certification-history-overview/

[11] ISO.(2014). Information technology security techniques: Information security management systems overview and vocabulary. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

[12] DCC. (2004-2015). Information security management: The ISO 27000 (ISO 27K) SERIES. Retrieved from http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s

[13] Gillies, A. (2011). The TQM Journal: Improving the quality of information security management systems with ISO27000. Retrieved from

[14] Cochran, M., & Patton, M.Q.(2002). A guide to using qualitative research methodology. Retrieved from https://evaluation.msf.org/sites/evaluation/files/a_guide_to_using_qualitative_research_methodology.pdf

Copyright © 2017 The authors

[15] Mora, M. (2010). Quantitative Vs. Qualitative Research: When to use which. Retrieved from http://www.surveygizmo.com/survey-blog/quantitative-qualitative-research/
[16] Colorado State University. (1993-2015). Case studies: Definition and overview. Retrieved from http://writing.colostate.edu/guides/page.cfm?pageid=1285&guideid=60
http://www.emeraldinsight.com/doi/abs/10.1108/17542731111139455
[17] Regoniel, P. (2010). What is the difference between the theoretical and the conceptual framework? Retrieved from https://college-college-life.knoji.com/what-is-the-difference-between-the-theoretical-framework-and-the-conceptual-framework/
[18] Vinz, S. (2016). The theoretical framework of a thesis: what and how? Retrieved from https://www.scribbr.com/thesis/the-theoretical-framework-of-a-thesis-what-and-how/
[19] Countrymeters.(2016). Namibia population. Retrieved from http://countrymeters.info/en/Namibia
[20] Office of the Prime Minister.(n.d). Task-enforcement. Retrieved from http://www.opm.gov.na/task-enforcement
[21] MICT. (n.d). About. Retrieved from https://www.facebook.com/pg/mictnamibia/about/?ref=page_internal
[22] CRAN.(n.d). About Us. Retrieved from http://www.cran.na/aboutus.html
[23]Rouse, M.(2006). Definition ISP -Internet service provider. Retrieved from http://searchwindevelopment.techtarget.com/definition/ISP
[24] ISO. (n.d). Namibia (NSI): Membership: Member body. Retrieved from http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1569
[25] AbuSaad, B., Saeed, F.A., Alghathbar, K., & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1104&context=ism
[26] IT NEWS AFRICA. (2016). Namibia still a top target for cybercriminals. Retrieved from http://www.itnewsafrica.com/2016/01/namibia-still-a-top-target-for-cybercriminals/
[27] Uudhila, J.M. (2016). CYBER SECURITY RISK MANAGEMENT AND THREAT CONTROL MODEL (CSRM-TCM): A STUDY CARRIED OUT TO ENHANCE THE PROTECTION OF INFORMATION IN THE NAMIBIAN PUBLIC SERVICE. Retrieved from https://repository.unam.edu.na/bitstream/handle/11070/1688/Uudhila_2016.pdf?sequence=1
[28] Kiilu, P.K., & Nzuki, D.M.(2015). Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review CPA. Retrieved from https://www.ijsr.net/archive/v5i12/ART20163327.pdf
[29] Kosutic, D. (n.d). ISO 27001 gap analysis vs. risk assessment. Retrieved from http://advisera.com/27001academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment/

APPENDIX D: Framework Evaluation Tool

Theoretical Framework Evaluation Tool: ISO/IEC 27000 Standards Implementation in Namibia

Dear Participants

This evaluation tool is part the study that is investigating the adoption and implementation of the ISO 27000 family of standard in local organisations. The purpose of this questionnaire is to collect information that will be used to determine the ISO 27000 family of standards security controls gap and design an ISO 27000 family of standards adoption framework that is specific to Namibia. The study is conducted by Diana J. Tjirare under the supervision of Dr. Fungai Bhunu Shava at the Namibia University of Science and Technology.

The questionnaire will require approximately 20 minutes of your time. You will complete the online questionnaire and submit it. The input you provide will be treated confidentially and only used towards the completion of the afore-mentioned study. Please answer the questionnaire as honestly and comprehensively as you can. There is no right or wrong answer to these questions – we are interested in your insight and opinion. All data will be used in summary form without reference to any individual. Participation in this research study is voluntary and no identification information will be required.

If you require any further information, please do not hesitate to contact me on 0855601000 or dkanikin@gmail.com.

Thank you for agreeing to take part in this research by completing this questionnaire.

Theoretical Framework ISO/IEC 27000 Standards Implementation in Namibia

According to Regoniel (2010) a theoretical framework provides a general representation of relationships between things in a given phenomenon. Additionally Regoniel (2010) said that a theoretical framework dwells on time tested theories that represent the findings of different investigations on how phenomena occur. The research project designed a theoretical framework that will inform the design of a policy framework to enable the implementation of security best practice in Namibia and a policy framework that will guide the adoption of ISO/IEC 27000 family of standards into security best practice in Namibia.

The survey results from different selected stakeholders and literature review were used for gap analysis to identify and validate the implementation extent of the ISO 27000 security standards. A theoretical framework was derived from the findings and is presented below.

The theoretical framework below shows the security of Namibia, possible mitigating strategies, the benefit of implementing the ISO/IEC 27000 standard, gap analysis scale, factors affecting the implementation and what still needs to be done to improve the security.

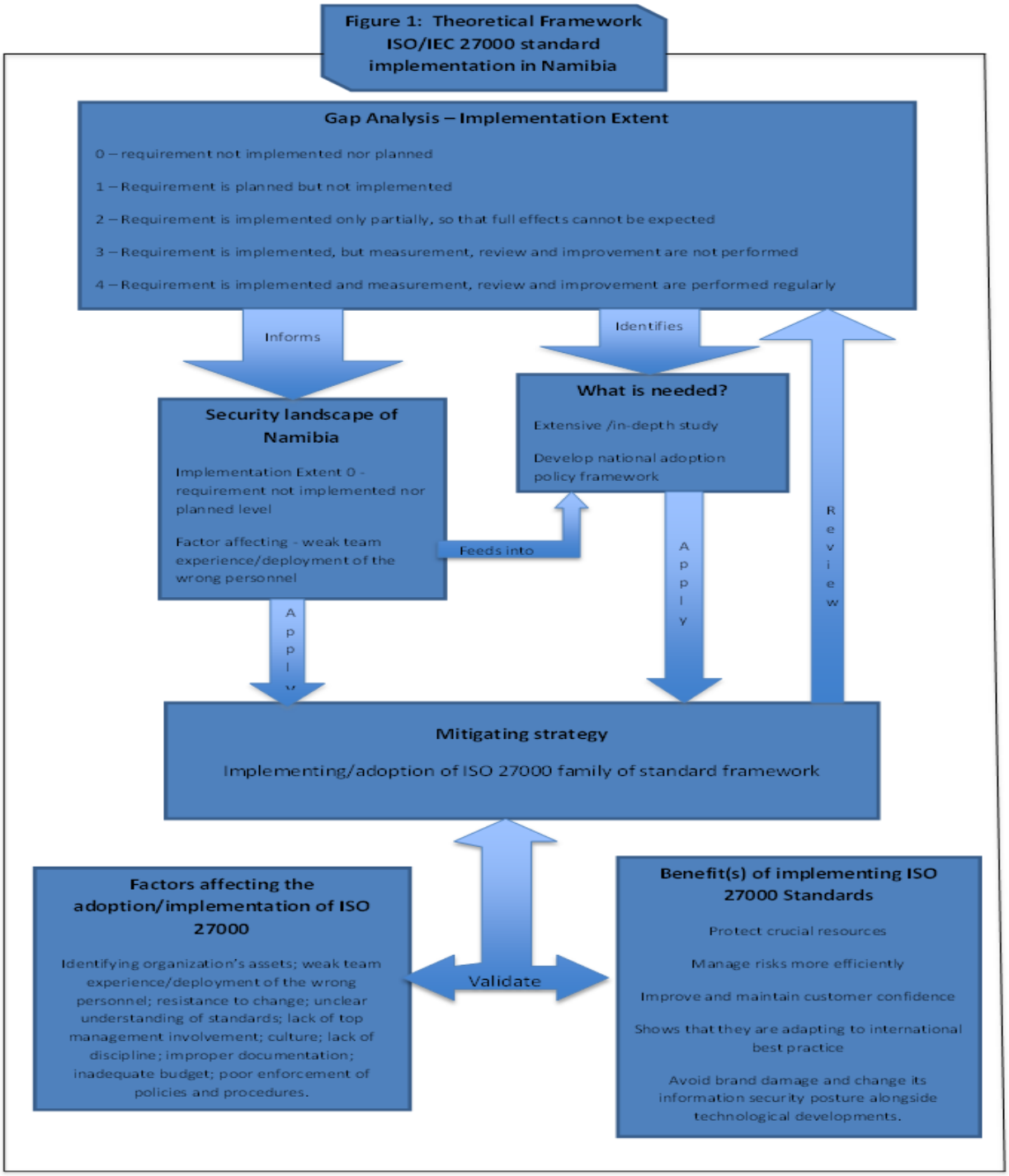


Figure 1: Theoretical Framework ISO/IEC 27000 standard implementation in Namibia
Gap Analysis – Implementation Extent
0 – requirement not implemented nor planned
1 – Requirement is planned but not implemented
2 – Requirement is implemented only partially, so that full effects cannot be expected
3 – Requirement is implemented, but measurement, review and improvement are not performed
4 – Requirement is implemented and measurement, review and improvement are performed regularly
Informs
Identifies
Security landscape of Namibia
Implementation Extent 0 - requirement not implemented nor planned level
Factor affecting - weak team experience/deployment of the wrong personnel
Feeds into
What is needed?
Extensive /in-depth study
Develop national adoption policy framework
Apply
Apply
Review
Mitigating strategy
Implementing/adoption of ISO 27000 family of standard framework
Validate
Factors affecting the adoption/implementation of ISO 27000
Identifying organization's assets; weak team experience/deployment of the wrong personnel; resistance to change; unclear understanding of standards; lack of top management involvement; culture; lack of discipline; improper documentation; inadequate budget; poor enforcement of policies and procedures.
Benefit(s) of implementing ISO 27000 Standards
Protect crucial resources
Manage risks more efficiently
Improve and maintain customer confidence
Shows that they are adapting to international best practice
Avoid brand damage and change its information security posture alongside technological developments.

Biographical Information

The purpose of this evaluation section is to collect biographical information of different stakeholders to differentiate the selected stakeholders.

Gender

- ☐ Male
- ☐ Female

Age Group

- ☐ 20 - 30
- ☐ 31 - 40
- ☐ 41 - 50
- ☐ 51 – 60

Position

- ☐ Head of Information Technology
- ☐ System Administrator
- ☐ Standard officer
- ☐ IT Technician
- ☐ Information Security Expert
- ☐ Others……

Information Security Years of Experiences

- ☐ 0 - 5
- ☐ 6 -10
- ☐ 11 - 20+

Organisation

- ☐ Office of the Prime Minister
- ☐ Ministry of Information and Communication Technology
- ☐ Communication Regulatory Authority of Namibia
- ☐ Namibia Institute of Standards
- ☐ Telecom Namibia
- ☐ Others……

Theoretical Framework Evaluation

How relevant are the factors below in the implementation of the ISO/IEC family of standards in your organisation?

A. Gap Analysis - Implementation Extent (Halkyn Security, 2013)

	Very Relevant	Relevant	Not Relevant	Least Relevant
Regularly reviewed Information Security policies (5.1.1- 5.1.2)				
Policy governing removable IT media (8.3.1)				
Formal procedure governing how removable IT media is disposed (8.3.2)				
Documented and communicated access control policy based on business requirements (9.1.1)				
Communicated policy document covering the organisations practices on how secret authentication information must be handled (9.3.1)				
Policy on the use of cryptographic controls (e.g encryption and decryption of information) (10.1.1)				
Processes to detect and prevent malware (12.2.1)				
Process and capacity to recover from a malware infection (12.2.1)				

Agreed backup policy that complies with relevant legal frameworks (12.3.1)				
Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)				
Appropriate event logs and sysadmin / sysop logs maintained and reviewed? (12.4.1- 12.4.3)				
Managers who are regularly instructed to review compliance with policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)				
Organisational policies that govern how information is transferred? (13.2.1)				
Information security function with documented, implemented validated, verified and maintained processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)				
Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)				
Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)				
Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)				
Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)				
Formal disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)				

Formal disciplinary process communicated to all employees (7.2.3)				
Documented process for terminating or changing employment duties relate to information security(7.3.1)				
Background verification checks carried out on all new employees? (7.1.1)				
Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)				
Are managers (of all levels) engaged in driving security within the business? (7.2.1)				
Process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role? (9.2.5 - 9.2.6)				

B. Security landscape of Namibia

	Very Relevant	Relevant	Not Relevant	Least Relevant
Determining the implementation extent of the standard				
Determining the factors that affect the implementation of the standard				

C. What is needed?

	Very Relevant	Relevant	Not Relevant	Least Relevant
Extensive/in-depth study of the				

standard				
Development of national adoption policy frameworks				

D. Mitigating strategy

	Very Relevant	Relevant	Not Relevant	Least Relevant
Implementation or adoption of ISO 27000 family of standard framework				

E. Factors affecting the adoption of ISO/IEC 27000 Standards

	Very Relevant	Relevant	Not Relevant	Least Relevant
Technical Team experience				
Deployment of the right IT personnel				
Willingness to change				
Clear understanding of standards				
Top management involvement				
Organisational information security Culture				
Employees discipline towards information security				
Proper Information Security documentation				
Inadequate IT budget				
Identifying organization's IT assets				
Poor enforcement of IT policies and procedures				

F. Benefits of implementing ISO 27000 family of standards

	Very Relevant	Relevant	Not Relevant	Least Relevant
Protect crucial resources				
Managing risks more efficiently				
Improving and maintaining customer confidence				
Benchmarking to international best practices				
Avoid brand damage and change its information security posture alongside technological developments.				

Any other comments:

…….

Theoretical Framework Evaluation

Which factors are important in the implementation of the ISO/IEC 27000 family of Standards in Namibia?

A. Gap Analysis - Implementation Extent (Halkyn Security, 2013)

	Very Relevant	Relevant	Not Relevant	Least Relevant
Regularly reviewed Information Security policies (5.1.1-5.1.2)				
Policy governing removable IT media (8.3.1)				
Formal procedure governing how removable IT media is disposed (8.3.2)				
Documented and communicated access control policy based on business requirements (9.1.1)				
Communicated policy document covering the organisations practices in how secret authentication information must be handled (9.3.1)				
Policy on the use of cryptographic controls (e.g encryption and decryption of information) (10.1.1)				
Processes to detect and prevent malware (12.2.1)				
Process and capacity to recover from a malware infection (12.2.1)				
Agreed backup policy that complies with relevant legal frameworks (12.3.1)				
Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)				
Appropriate event logs and sysadmin / sysop logs maintained and reviewed? (12.4.1- 12.4.3)				
Managers who are regularly instructed to review compliance with policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)				
Organisational policies that govern how information is transferred? (13.2.1)				
Information security function with documented, implemented validated, verified and maintained processes				

to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)				
Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)				
Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)				
Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)				
Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)				
Formal disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)				
Formal disciplinary process communicated to all employees (7.2.3)				
Documented process for terminating or changing employment duties relate to information security(7.3.1)				
Background verification checks carried out on all new employees? (7.1.1)				
Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)				
Are managers (of all levels) engaged in driving security within the business? (7.2.1)				
Process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role? (9.2.5 - 9.2.6)				

B. Security landscape of Namibia

	Very Relevant	Relevant	Not Relevant	Least Relevant
Determining the implementation extent of the standard				
Determining the factors that affect the implementation of the standard				

C. What is needed?

	Very Relevant	Relevant	Not Relevant	Least Relevant
Extensive/in-depth study of the standard				
Development of national adoption policy frameworks				

D. Mitigating strategy

	Very Relevant	Relevant	Not Relevant	Least Relevant
Implementation or adoption of ISO 27000 family of standard framework				

E. Factors affecting the adoption of ISO/IEC 27000 Standards

	Very Relevant	Relevant	Not Relevant	Least Relevant
Technical Team experience				
Deployment of the right IT personnel				
Willingness to change				
Clear understanding of standards				
Top management involvement				
Culture				
Lack of discipline				
Improper documentation				
Inadequate IT budget				
Identifying organization's IT assets				
Poor enforcement of IT policies and procedures				

F. Benefits of implementing ISO 27000 family of standards

	Very Relevant	Relevant	Not Relevant	Least Relevant
Protect crucial resources				
Managing risks more efficiently				
Improving and maintaining customer confidence				
Benchmarking to international best practices				
Avoid brand damage and change its information security posture alongside technological developments.				

Any other comments:

……

Information Security Controls

Information Security Controls	**Description**
Information Security Policies	Management direction and support for information security according to the organisations requirements and laws and regulations.
Operations Security	Deals with information backup, logging, monitoring and protection from malware.
Cryptography	Appropriate information encryption and decryption to protect its confidentiality, authenticity and integrity.
System acquisition, development and maintenance	Deals with security requirements of information system and the protection of test data
Asset Management	To prevent unauthorized access of information stored in media and ensure that information is protected in accordance to its priority in the organisation
Human Resource Security	Internal and external human resource security management prior to employment, during employment and when terminating employment
Compliance	The implementation and operation of information security according to organizational policies and procedures.
Access Control	Limit access to information, ensure authorized user access to systems and service, and make sure users are responsible for protecting their authentication information.
Organisation of information security	The administrative of a management framework,

	security of teleworking and use of mobile devices to promote effective management.
Communication Security	Deals with the protection of information in networks and maintain the security of information transfer.

Please rate the importance of the security controls:

	Very Important	Important	Not Important	Least Important
Information Security Policies				
Operations Security				
Cryptography				
System acquisition, development and maintenance				
Asset Management				
Human Resource Security				
Compliance				
Access Control				
Organisation of information security				
Communication Security				

Please rate the relevance of the security controls:

	Very Relevant	Relevant	Not Relevant	Least Relevant
Information Security Policies				
Operations Security				
Cryptography				
System acquisition, development and maintenance				
Asset Management				
Human Resource Security				
Compliance				
Access Control				
Organisation of information security				
Communication Security				

Overall Framework Evaluation

Please validate the whole theoretical framework

	Strongly Agree	Agree	Disagree	Strongly Disagree
Efficient				
Operational				
Well designed and developed				
Relevant and needed				
Useful and valuable				
Adaptable and customisable				
Requires a lot of improvement				

Any other comments:

……

Thank you for your participation

APPENDIX E: Framework Evaluation Results

A. Gap Analysis - Implementation Extent

Table 1: Gap Analysis - matching and contradicting results of relevant responses

Security Controls	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
1. Regularly reviewed Information Security policies (5.1.1- 5.1.2)	6	0	3	0	0	2	0	0
2. Policy governing removable IT media (8.3.1)	4	0	5	0	0	2	0	0
3. Formal procedure governing how removable IT media is disposed (8.3.2)	3	0	5	0	0	2	0	1
4. Documented and communicated access control policy based on business requirements	5	0	6	0	0	0	0	0

(9.1.1)								
5. Communicated policy document covering the organisations practices on how secret authentication information must be handled (9.3.1)	5	0	4	0	0	1	0	1
6. Policy on the use of cryptographic controls (e.g encryption and decryption of information) (10.1.1)	6	0	3	0	0	1	0	1
7. Processes to detect and prevent malware (12.2.1)	7	0	4	0	0	0	0	0
8. Process and capacity to recover from a malware infection	7	0	3	0	0	1	0	0

(12.2.1)								
9. Agreed backup policy that complies with relevant legal frameworks (12.3.1)	7	0	4	0	0	0	0	0
10. Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)	7	0	1	0	0	3	0	0
11. Appropriate event logs and sysadmin / sysop logs maintained and reviewed? (12.4.1- 12.4.3)	5	0	2	0	0	3	0	1
12. Managers who are regularly instructed to review compliance with	4	0	3	0	1	1	1	1

policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)								
13. Organisational policies that govern how information is transferred? (13.2.1)	6	0	2	0	0	2	0	1
14. Information security function with documented, implemented Matchingated, verified and maintained processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)	5	0	2	0	0	3	0	1
15. Media protected against	3	0	4	0	0	4	0	0

unauthorised access, misuse or corruption while transporting (8.3.3)								
16. Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)	5	0	3	0	0	3	0	0
17. Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)	5	0	4	0	1	1	0	0
18. Employees, contractors and 3rd party users regularly given security awareness	3	0	1	0	0	4	1	2

training appropriate to their role and function within the organization (7.2.2)								
19. Formal disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)	3	0	6	0	0	1	0	1
20. Formal disciplinary process communicated to all employees (7.2.3)	3	0	5	0	0	2	0	1
21. Documented process for terminating or changing employment duties relate to	5	0	2	0	0	4	0	0

information security(7.3.1)								
22. Background verification checks carried out on all new employees? (7.1.1)	4	0	1	1	2	2	0	1
23. Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)	5	0	4	0	0	1	0	1
24. Are managers (of all levels) engaged in driving security within the business? (7.2.1)	4	0	4	0	0	2	0	1
25. Process to ensure user access rights are removed on termination of employment or contract, or	8	0	3	0	0	0	0	0

adjusted upon change of role? (9.2.5 - 9.2.6)								

Table 2: Gap Analysis - Matching and contradicting results of important responses

Security Controls	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
1. Regularly reviewed Information Security policies (5.1.1- 5.1.2)	9	2	0	0	0	0	0	0
2. Policy governing removable IT media (8.3.1)	7	1	2	1	0	0	0	0
3. Formal procedure governing how removable IT media is disposed (8.3.2)	5	1	3	2	0	0	0	0
4. Documented and	8	0	3	0	0	0	0	0

communicated access control policy based on business requirements (9.1.1)								
5. Communicated policy document covering the organisations practices on how secret authentication information must be handled (9.3.1)	8	1	1	1	0	0	0	0
6. Policy on the use of cryptographic controls (e.g encryption and decryption of information) (10.1.1)	6	1	3	1	0	0	0	0
7. Processes to detect and	10	0	1	0	0	0	0	0

prevent malware (12.2.1)								
8. Process and capacity to recover from a malware infection (12.2.1)	8	0	2	1	0	0	0	0
9. Agreed backup policy that complies with relevant legal frameworks (12.3.1)	10	0	1	0	0	0	0	0
10. Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)	8	1	0	2	0	0	0	0
11. Appropriate event logs	6	2	1	2	0	0	0	0

and sysadmin / sysop logs maintained and reviewed? (12.4.1-12.4.3)								
12. Managers who are regularly instructed to review compliance with policy and procedures within their area of responsibility ? (18.2.1 - 18.2.2)	5	0	2	2	2	0	0	0
13. Organisational policies that govern how information is transferred? (13.2.1)	7	2	1	1	0	0	0	0
14. Information security	7	4	0	0	0	0	0	0

function with documented, implemented Matchingated, verified and maintained processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)								
15. Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)	6	3	1	1	0	0	0	0
16. Security policies on the use of information transfer while using	8	2	0	1	0	0	0	0

electronic messaging systems? (13.2.3)								
17. Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)	7	1	1	0	0	0	2	0
18. Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)	4	4	0	2	0	0	1	0
19. Formal	7	2	2	0	0	0	0	0

disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)								
20. Formal disciplinary process communicated to all employees (7.2.3)	7	2	1	1	0	0	0	0
21. Documented process for terminating or changing employment duties relate to information security(7.3.1)	7	1	0	3	0	0	0	0
22.	5	1	2	0	2	1	0	0

Background verification checks carried out on all new employees? (7.1.1)								
23. Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)	7	0	2	2	0	0	0	0
24. Are managers (of all levels) engaged in driving security within the business? (7.2.1)	6	2	2	1	0	0	0	0
25. Process to ensure user access rights are removed on	10	0	1	0	0	0	0	

termination of employment or contract, or adjusted upon change of role? (9.2.5 - 9.2.6)								

Table 3: Gap Analysis - Total percentage of matching relevant responses

Security Controls	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
1. Regularly reviewed Information Security policies (5.1.1- 5.1.2)	9	6	67	3	33	0	0	0	0
2. Policy governing removable IT media (8.3.1)	9	4	44	5	56	0	0	0	0
3. Formal procedure governing how removable IT media is disposed (8.3.2)	8	3	37.5	5	62.5	0	0	0	0
4. Documented and communicated access control policy based on business requirements (9.1.1)	11	5	45	6	55	0	0	0	0
5. Communicated policy document	9	5	56	4	44	0	0	0	0

covering the organisations practices in how secret authentication information must be handled (9.3.1)									
6. Policy on the use of cryptographic controls (e.g encryption and decryption of information) (10.1.1)	9	6	67	3	33	0	0	0	0
7. Processes to detect and prevent malware (12.2.1)	11	7	64	4	36	0	0	0	0
8. Process and capacity to recover from a malware infection (12.2.1)	10	7	70	3	30	0	0	0	0
9. Agreed backup policy that complies with relevant legal frameworks (12.3.1)	11	7	64	4	36	0	0	0	0
10. Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)	8	7	87.5	1	12.5	0	0	0	0
11. Appropriate event logs and sysadmin /	7	5	71	2	29	0	0	0	0

sysop logs maintained and reviewed? (12.4.1- 12.4.3)									
12. Managers who are regularly instructed to review compliance with policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)	9	4	44.44	3	33.33	1	11.11	1	11.11
13. Organisational policies that govern how information is transferred? (13.2.1)	8	6	75	2	25	0	0	0	0
14. Information security function with documented, implemented Matchingated, verified and maintained processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)	7	5	71	2	29	0	0	0	0
15. Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)	7	3	43	4	57	0	0	0	0

16. Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)	8	5	62.5	3	37.5	0	0	0	0
17. Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)	10	5	50	4	40	1	10	0	0
18. Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)	5	3	60	1	20	0	0	1	20
19. Formal disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)	9	3	33	6	67	0	0	0	0

20. Formal disciplinary process communicated to all employees (7.2.3)	8	3	37.5	5	62.5	0	0	0	0
21. Documented process for terminating or changing employment duties relate to information security(7.3.1)	7	5	71	2	29	0	0	0	0
22. Background verification checks carried out on all new employees? (7.1.1)	7	4	57	1	14	2	29	0	0
23. Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)	9	5	56	4	44	0	0	0	0
24. Are managers (of all levels) engaged in driving security within the business? (7.2.1)	8	4	50	4	50	0	0	0	0
25. Process to ensure user access rights are removed on termination of employment or contract, or adjusted	11	8	73	3	27	0	0	0	0

upon change of role? (9.2.5 - 9.2.6)									

Table 4: Gap Analysis - Total percentage of matching important responses

Security Controls	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
1. Regularly reviewed Information Security policies (5.1.1- 5.1.2)	9	9	100	0	0	0	0	0	0
2. Policy governing removable IT media (8.3.1)	9	7	78	2	22	0	0	0	0
3. Formal procedure governing how removable IT media is disposed (8.3.2)	8	5	62.5	3	37.5	0	0	0	0
4. Documented and communicated access control policy based on business requirements (9.1.1)	11	8	73	3	27	0	0	0	0
5. Communicated policy document covering the organisations practices in how secret authentication information must be handled (9.3.1)	9	8	89	1	11	0	0	0	0
6. Policy on the use of cryptographic controls (e.g encryption and decryption of	9	6	67	3	33	0	0	0	0

information) (10.1.1)									
7. Processes to detect and prevent malware (12.2.1)	11	10	91	1	9	0	0	0	0
8. Process and capacity to recover from a malware infection (12.2.1)	10	8	80	2	20	0	0	0	0
9. Agreed backup policy that complies with relevant legal frameworks (12.3.1)	11	10	91	1	9	0	0	0	0
10. Event logs and sysadmin / sysop logs logging facilities that are protected against tampering and unauthorised access (12.4.2)	8	8	100	0	0	0	0	0	0
11. Appropriate event logs and sysadmin / sysop logs maintained and reviewed? (12.4.1- 12.4.3)	7	6	86	1	14	0	0	0	0
12. Managers who are regularly instructed to review compliance with policy and procedures within their area of responsibility? (18.2.1 - 18.2.2)	9	5	56	2	22	2	22	0	0
13. Organisational policies that govern how information is transferred? (13.2.1)	8	7	87.5	1	12.5	0	0	0	0
14. Information security function with documented, implemented Matchingated, verified and maintained	7	7	100	0	0	0	0	0	0

processes to maintain continuity of service during an unfavourable situation (17.1.2 - 17.1.3)									
15. Media protected against unauthorised access, misuse or corruption while transporting (8.3.3)	7	6	86	1	14	0	0	0	0
16. Security policies on the use of information transfer while using electronic messaging systems? (13.2.3)	8	8	100	0	0	0	0	0	0
17. Is there a formal user access provisioning process in place to assign access rights for all user types and services? (9.2.1 – 9.2.2)	10	7	70	1	10	0	0	2	20
18. Employees, contractors and 3rd party users regularly given security awareness training appropriate to their role and function within the organization (7.2.2)	5	4	80	0	0	0	0	1	20
19. Formal disciplinary process which allows the organization to take action against employees who have committed an information security breaches (7.2.3)	9	7	78	2	22	0	0	0	0
20. Formal disciplinary process communicated to all	8	7	87.5	1	12.5	0	0	0	0

employees (7.2.3)									
21. Documented process for terminating or changing employment duties relate to information security(7.3.1)	7	7	100	0	0	0	0	0	0
22. Background verification checks carried out on all new employees? (7.1.1)	9	5	56	2	22	2	22	0	0
23. Employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? (7.1.2)	9	7	78	2	22	0	0	0	0
24. Are managers (of all levels) engaged in driving security within the business? (7.2.1)	8	6	75	2	25	0	0	0	0
25. Process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role? (9.2.5 - 9.2.6)	11	10	91	1	9	0	0	0	0

B. Security landscape of Namibia

Table 5: Security landscape of Namibia - Matching and contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Determining the implementation extent of the standard	5	0	5	0	0	1	0	0
Determining the factors that affect the implementation of the standard	4	0	4	1	0	1	1	0

Table 6: Security landscape of Namibia - Matching and contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Determining the implementation extent of the standard	10	1	0	0	0	0	0	0
Determining the factors	9	1	0	0	0	0	0	1

that affect the implementation of the standard								

Table 7: Security landscape of Namibia - Total percentage of matching relevant responses

	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Determining the implementation extent of the standard	10	5	50	5	50	0	0	0	0
Determining the factors that affect the implementation of the standard	9	4	44.4	4	44.4	0	0	1	11.1

Table 8: Security landscape of Namibia - Total percentage of matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Determining the	10	10	100	0	0	0	0	0	0

implementation extent of the standard									
Determining the factors that affect the implementation of the standard	9	9	100	0	0	0	0	0	0

C. What is needed?

Table 9: What is needed - Matching and contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Extensive /in-depth study of the standard	9	0	2	0	0	0	0	0
Development of national adoption policy frameworks	9	0	1	0	0	0	0	1

Table 10: What is needed - Matching and contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Extensive /in-depth study of the standard	10	0	1	0	0	0	0	0
Development of national adoption policy frameworks	9	0	1	1	0	0	0	0

Table 11: What is needed - Total percentage of matching relevant responses

	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Extensive/in-depth study of the standard	11	9	81.8	2	18.18	0	0	0	0
Development of national adoption	10	9	90	1	10	0	0	0	0

policy frameworks									

Table 12: What is needed - Total percentage of matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Extensive/in-depth study of the standard	11	10	90.9	1	9.09	0	0	0	0
Development of national adoption policy frameworks	10	9	90	1	10	0	0	0	0

D. Mitigating strategy

Table 13 Mitigating strategy - Matching/Contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Implementation or adoption of ISO 27000 family of standard framework	7	0	4	0	0	0	0	0

Table 14 Mitigating strategy - Matching/Contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Implementation or adoption of ISO 27000 family of standard framework	10	0	1	0	0	0	0	0

Table 15 Mitigating strategy - Total percentage of Matching relevant responses

	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Implementation or adoption of ISO 27000 family of standard framework	11	7	63.6	4	36.4	0	0	0	0

Table 16: Mitigating strategy - Total percentage of Matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Implementation or adoption of ISO 27000 family of standard framework	11	10	90.9	1	9.1	0	0	0	0

E. Factors affecting the adoption of ISO/IEC 27000 Standards

Table 17: Factors affecting the adoption of the Standard - Matching/Contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Technical Team experience	7	0	3	0	0	1	0	0
Deployment of the right IT personnel	8	0	2	0	0	0	0	1
Willingness to change	7	0	1	0	0	1	0	2
Clear understanding of standards	7	0	3	0	0	1	0	0
Top management involvement	8	0	2	0	0	0	0	1
Organisational informatio	8	0	2	0	0	0	1	0

n security Culture								
Employees lack of discipline towards informatio n security	6	0	4	0	0	0	1	0
Improper Informatio n Security documentation	7	0	4	0	0	0	0	0
Inadequat e IT budget	5	0	3	0	0	0	2	1
Identifying organizati on's IT assets	9	0	2	0	0	0	0	0
Appropria te enforceme nt of IT policies and procedure s	7	0	2	0	0	1	0	1

Table 18: Factors affecting the adoption of the standard - Matching/Contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Technical Team experience	9	0	1	1	0	0	0	0
Deployment of the right IT personnel	8	1	2	0	0	0	0	0
Willingness to change	6	1	2	2	0	0	0	0
Clear understanding of standards	8	1	2	0	0	0	0	0
Top management involvement	8	1	2	0	0	0	0	0
Organisational information security Culture	9	0	1	0	0	0	1	0
Employees lack of	11	0	0	0	0	0	0	0

discipline towards information security								
Improper Information Security documentation	10	0	1	0	0	0	0	0
Inadequate IT budget	7	1	1	0	0	0	2	0
Identifying organization's IT assets	10	0	1	0	0	0	0	0
Appropriate enforcement of IT policies and procedures	8	2	1	0	0	0	0	0

Table 19: Factors affecting the adoption of the standard - Total percentage of Matching relevant responses

	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Technical Team experience	10	7	70	3	30	0	0	0	0
Deployment of the right IT personnel	10	8	80	2	20	0	0	0	0
Willingness to change	8	7	87.5	1	12.5	0	0	0	0
Clear understanding of standards	10	7	70	3	30	0	0	0	0
Top management involvement	10	8	80	2	20	0	0	0	0
Organisational information security Culture	11	8	72.73	2	18.18	0	0	1	9.09
Employees lack of discipline towards information	11	6	54.55	4	36.36	0	0	1	9.09

security									
Improper Information Security documentation	11	7	63.64	4	36.36	0	0	0	0
Inadequate IT budget	10	5	50	3	30	0	0	2	20
Identifying organization's IT assets	11	9	81.82	2	18.18	0	0	0	0
Appropriate enforcement of IT policies and procedures	9	7	77.78	2	22.22	0	0	0	0

Table 20: Factors affecting the adoption of the standard - Total percentage of matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Technical Team experience	10	9	90	1	10	0	0	0	0
Deployment of the right IT	10	8	80	2	20	0	0	0	0

personnel									
Willingness to change	8	6	75	2	25	0	0	0	0
Clear understanding of standards	10	8	80	2	20	0	0	0	0
Top management involvement	10	8	80	2	20	0	0	0	0
Organisational information security Culture	11	9	81.82	1	9.09	0	0	1	9.09
Employees lack of discipline towards information security	11	11	100	0	0	0	0	0	0
Improper Information Security documentation	11	10	90.91	1	9.09	0	0	0	0
Inadequate IT budget	8	7	87.5	1	12.5	0	0	2	25
Identifying organization's IT assets	11	10	90.91	1	9.09	0	0	0	0
Appropriate enforcement	9	8	88.89	1	11.11	0	0	0	0

of IT policies and procedures									

F. Benefits of implementing ISO/IEC 27000 family of standards

Table 21: Benefits of implementing ISO/IEC 27000 family of standards - Matching/Contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Protect crucial resources	10	0	1	0	0	0	0	0
Managing risks more efficiently	8	0	3	0	0	0	0	0
Improving and maintaining customer confidence	6	0	4	1	0	0	0	0
Benchmarking to international best practices	7	0	4	0	0	0	0	0
Avoid	7	0	3	0	1	0	0	0

brand damage and change its information security posture alongside technological developments.								

Table 22: Benefits of implementing ISO/IEC 27000 family of standards - Matching/Contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Protect crucial resources	10	0	1	0	0	0	0	0
Managing risks more efficiently	9	0	2	0	0	0	0	0
Improving and maintaining customer confidenc	8	0	2	0	0	1		0

e								
Benchmarking to international best practices	7	0	4	0	0	0	0	0
Avoid brand damage and change its information security posture alongside technological developments.	8	0	2	0	1	0	0	0

Table 23: Benefits of implementing ISO/IEC 27000 family of standards - Total percentage of matching relevant responses

	Number of responses per category								
	Total Matching Response	Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Protect crucial	11	10	90.91	1	9.09	0	0	0	0

resources									
Managing risks more efficiently	11	8	72.73	3	27.27	0	0	0	0
Improving and maintaining customer confidence	10	6	60	4	40	0	0	0	0
Benchmarking to international best practices	11	7	63.64	4	36.36	0	0	0	0
Avoid brand damage and change its information security posture alongside technological developments.	11	7	63.64	3	27.27	1	9.09	0	0

Table 24: Benefits of implementing ISO/IEC 27000 family of standards - Total percentage of Matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Protect crucial resources	11	10	90.91	1	9.09	0	0	0	0
Managing risks more efficiently	11	9	81.82	2	18.18	0	0	0	0
Improving and maintaining customer confidence	10	8	80	2	20	0	0	0	0
Benchmarking to international best practices	11	7	63.64	4	36.36	0	0	0	0
Avoid brand damage and change its information security posture alongside	11	8	72.73	2	18.18	1	9.09	0	0

technological developments.									

Information Security Controls

Table 25: Security Controls - Matching/Contradicting results of important responses

	Number of responses per category							
	Very Important		Important		Not Important		Least Important	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Information Security Policies	10	0	1	0	0	0	0	0
Operations Security	7	0	3	0	0	0	1	0
Cryptography	4	0	6	0	0	0	1	0
System acquisition, development and maintenance	6	0	4	0	0	0	1	0
Asset Management	7	0	4	0	0	0	0	0
Human	8	0	2	0	0	0	1	0

Resource Security								
Compliance	9	0	2	0	0	0	0	0
Access Control	11	0	0	0	0	0	0	0
Organisation of information security	11	0	0	0	0	0	0	0
Communication Security	9	0	1	1	0	0	0	0

Table 26: Security Controls - Matching/Contradicting results of relevant responses

	Number of responses per category							
	Very Relevant		Relevant		Not Relevant		Least Relevant	
	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting	Matching	Contradicting
Information Security Policies	8	0	3	0	0	0	0	0
Operations Security	7	0	3	0	0	0	1	0
Cryptography	5	0	5	0	0	0	1	0
System	8	0	2	0	0	0	1	0

acquisition, development and maintenance								
Asset Management	5	0	6	0	0	0	0	0
Human Resource Security	4	0	6	0	0	0	1	0
Compliance	8	0	3	0	0	0	0	0
Access Control	9	0	2	0	0	0	0	0
Organisation of information security	9	0	2	0	0	0	0	0
Communication Security	10	0	0	0	0	1	0	0

Table 27: Security Controls - Total percentage of matching important responses

	Number of responses per category								
	Total Matching Response	Very Important		Important		Not Important		Least Important	
		Matching	%	Matching	%	Matching	%	Matching	%
Information Security Policies	11	10	90.91	1	9.09	0	0	0	0
Operations Security	11	7	63.64	3	27.27	0	0	1	9.09
Cryptography	11	4	36.36	6	54.55	0	0	1	9.09
System acquisition, development and maintenance	11	6	54.55	4	36.36	0	0	1	9.09
Asset Management	11	7	63.64	4	36.36	0	0	0	0
Human Resource Security	11	8	72.73	2	18.18	0	0	1	9.09
Compliance	11	9	81.82	2	18.18	0	0	0	0
Access Control	11	11	100	0	0	0	0	0	0

Organisation of information security	11	11	100	0	0	0	0	0	0
Communication Security	10	9	90	1	10	0	0	0	0

Table 28: Security Controls - Total percentage of Matching relevant responses

	Number of responses per category								
		Very Relevant		Relevant		Not Relevant		Least Relevant	
		Matching	%	Matching	%	Matching	%	Matching	%
Information Security Policies	11	8	72.73	3	27.27	0	0	0	0
Operations Security	11	7	63.64	3	27.27	0	0	1	9.09
Cryptography	11	5	45.45	5	45.45	0	0	1	9.09
System acquisition, development and maintenance	11	8	72.73	2	18.18	0	0	1	9.09
Asset Management	11	5	45.45	6	54.55	0	0	0	0
Human Resource Security	11	4	36.36	6	54.55	0	0	1	9.09
Compliance	11	8	72.73	3	27.27	0	0	0	0
Access	11	9	81.82	2	18.18	0	0	0	0

Control									
Organisation of information security	11	9	81.82	2	18.18	0	0	0	0
Communication Security	10	10	100	0	0	0	0	0	0

APPENDIX F: Language Editor

ACET Consultancy
Anenyasha Communication, Editing and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk / nelsonmlambo@icloud.com

25 June 2018

To whom it may concern

LANGUAGE EDITING – DIANA J. TJIRARE

This letter serves to confirm that a Master of Computer Science thesis entitled "Designing a national adoption policy framework for ISO/IEC 27000 standards implementation in Namibia" by Diana J. Tjirare was submitted to me for language editing.

The thesis was professionally edited and track changes and suggestions were made in the document, which if followed by Ms Diana J. Tjirare will result in a thesis with a high standard of English.

Yours faithfully

NMlambo
Dr N. Mlambo

ACET Consultancy
Anenyasha Communication, Editing & Training
Box 95509 Soweto, Windhoek, Namibia
Cells: (+264) 814218613 or 0814234235
Email: mlambons@yahoo.co.uk
nelsonmlambo@icloud.com

PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics