# TOWARDS A WIRELESS LOCAL AREA NETWORK SECURITY CONTROL FRAMEWORK FOR SMALL, MEDIUM AND MICRO ENTERPRISES IN SOUTH AFRICA

By

**PAUL VAN DE HAAR**

Submitted in fulfilment of the requirements for the degree

Magister Technologiae

in

INFORMATION TECHNOLOGY

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT

AND INFORMATION TECHNOLOGY

at the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Professor Johan van Niekerk

December 2014

The financial assistance of the National Research Foundation (NRF) for this research study is hereby acknowledged. The opinions expressed and conclusions drawn are those of the author and should not necessarily be attributed to the NRF.

**Declaration by student**

| | |
|---|---|
| **NAME:** | **Paul van de Haar** |
| **STUDENT NUMBER:** | **206006381** |
| **QUALIFICATION:** | **MTech IT** |

**TITLE OF PROJECT: TOWARDS A WIRELESS LOCAL AREA NETWORK SECURITY CONTROL FRAMEWORK FOR SMALL, MEDIUM AND MICRO ENTERPRISES IN SOUTH AFRICA**

DECLARATION:

I hereby declare that the above-mentioned dissertation is my own work and that it has not previously been submitted for assessment to another university or for another qualification.

SIGNATURE: _____

DATE: _____

## Abstract

There is little literature available that is specific to the use of wireless local area network (WLAN) security among small, medium and micro enterprises (SMMEs) in South Africa.

This research study developed a framework which may be used by SMMEs for the purposes of securing their WLANs. In view of the fact that the aim of the study was to develop a system for improving information technology security, the study followed a design science approach. A literature review was conducted on security control framework standards and WLAN technologies. The needs of SMMEs regarding WLANs were also established.

The result of this process was an artefact in the form of a WLAN Security Control Framework for securing WLANs for SMMEs in South Africa. The suitability of the framework was validated by means of a focus group.

**Keywords**: Framework, WLANs, SMMEs, information security

## Acknowledgements

I would like to thank the following people/organisations:

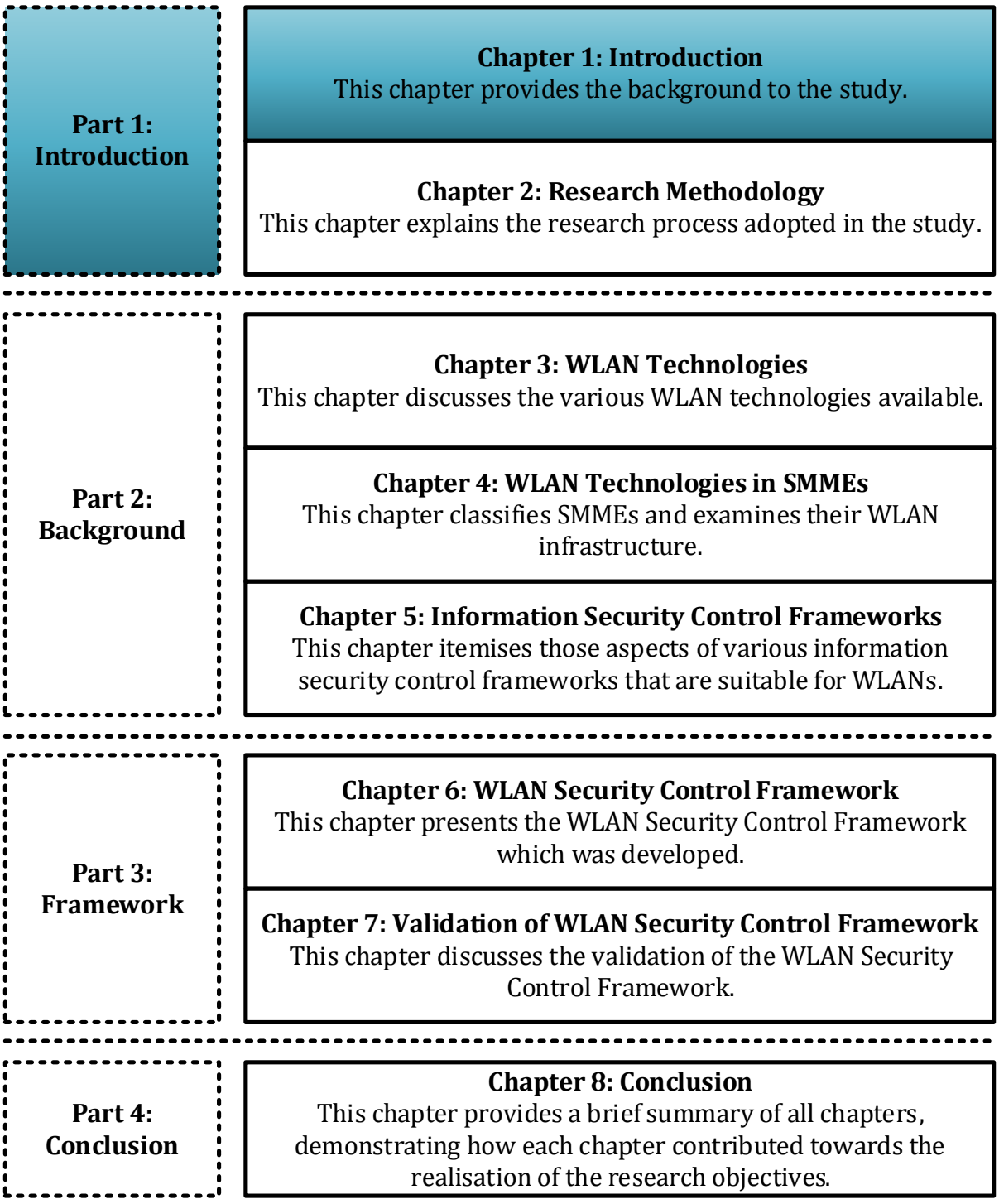
- My promoter, Professor Johan van Niekerk, for his guidance which has played a key role in the completion of this dissertation
- My wife, Jacky van de Haar, for all the love and support she has given me over the last few years
- My family, for their constant, positive input and motivation
- The Nelson Mandela Metropolitan University and the National Research Foundation for the financial support I received
- God, who made it all possible

# Table of Contents

## Table of Figures

## Table of Tables

# 1 Introduction



## 1.1 Introduction

This chapter contains the introduction to the research study. Section 1.2 describes the rationale behind the study and section 1.3 presents the problem statement. This is followed by the research questions in section 1.4 and the research objectives in section 1.5. Section 1.6 summarises the research process, while section 1.7 describes the scope and delineation of the study. As discussed in section 1.8, there were no ethical considerations to be observed. The layout of chapters is presented in section 1.9.

## 1.2 Rationale

Information technology is important for the businesses of today because this is the information age, with information and its uses permeating modern life. Information technology is required to store, control and manipulate a company's information, which has several benefits for the company concerned. However, if the information technology functions are not implemented properly this may impact negatively on the company concerned. Information technology enables communication and creates opportunities, especially for small businesses which are able to transact with larger organisations as a result of their ability to communicate electronically (Tapscott & Caston, 1993; Powell & Dent-Micallef, 1997).

However, the networking which is required to facilitate communication demands substantial investment, for example, a wired local area network involves overheads which include the laying of cables to each device connected. However, in the case of wireless local area networks (WLANs) it is possible to add several additional devices and connect these devices easily without extra overheads being incurred (McCullough, 2001).

In view of the importance of information and technology resources, it is of the utmost important that these resources are protected to prevent any loss of business. Companies may use international information security framework standards such as the Control Objectives for Information and Related Technology (COBIT) 5 for Information Security (ISACA, 2012), the International Organisation for Standardisation and the International Electro-Technical Commission (ISO/IEC 27002 (2005), Information Security Forum (ISF) Standard of Good Practice 2012 (Information Security Forum, 2012), Information Technology Infrastructure Library (ITIL) (Von Bon, 2007), and the National Institute of

Standards and Technology (NIST) Special Publication (SP) 800-100 (NIST, 2006) to protect their information and technology resources.

However, these standards may not necessarily be appropriate for small, medium and micro enterprises (SMMEs) in South Africa. There is little known about the way in which SMMEs protect their WLANs and, thus, a limited survey was conducted to establish whether SMMEs in South Africa currently use WLANs and how such networks are protected. The details of this survey are contained in Appendix A.

It emerged from the survey that WLANs were used widely by SMMEs. However, there was a lack of WLAN security controls. This was perceived as a problem and resulted in this research endeavour.

## 1.3 Problem Statement

Modern businesses are not able to compete in today's competitive business environment unless they have access to information technology resources and, specifically, to networking resources (Powell & Dent-Micallef, 1997). This is especially true for SMMEs because, in general, SMMEs do have no major information technology divisions in their companies to support high availability requirements. SMMEs often tend to use WLANs. However, this practice is accompanied by its own set of problems. It is essential that organisations protect themselves against the increasing threats that are exacerbated by Internet communications (Upfold & Sewry, 2005).

As mentioned above a preliminary survey was conducted to explore the WLAN security landscape in which SMMEs in South Africa operate. It was found that the majority of SMMEs do not have sufficient WLAN security controls in place.

This problem is exacerbated by the fact that SMMEs do not necessarily possess the resources or knowledge required to secure WLANs on their own and, for the majority of SMMEs, this task is considered to be both daunting and unachievable (Upfold & Sewry, 2005).

There does exist some guidance in the form of the international, information security, best practice control framework standards which were mentioned in the previous section. However, SMMEs do not necessarily have the financial resources available to purchase these standards while these standards are also not *specific* to WLANs and, more particularly, to the WLAN needs of SMMEs. Thus these standards are not necessarily

useful in the context of securing WLANs within SMMEs with SMMEs requiring guidance that is less complex and requires fewer resources to implement as compared to the standards mentioned above.

Thus, the problem which this dissertation addresses may be stated as follows:

*There exists a lack of guidance regarding the securing of Wireless Local Area Networks (WLANs) among small, medium, and micro enterprises (SMMEs) in South Africa.*

## 1.4 Research Questions

The main research question is as follows:

*What components are necessary for the creation of a WLAN security control framework specific to the needs of SMMEs in South Africa?*

The sub-research questions are as follows:

1. What are the needs of SMMEs with regard to WLAN security?
2. Which security control framework standards govern WLANs?
3. What components should form part of a WLAN Security Control Framework that will be specific to the needs of SMMEs in South Africa?

## 1.5 Research Objectives

The primary objective of this dissertation was to develop a framework that SMMEs could use to implement WLAN security. This framework, termed the WLAN Security Control Framework, was based on applicable security standards and best practices.

In order to achieve the primary research objective, it was necessary to realise the following sub-objectives:

- Determine the needs of SMMEs with regard to WLAN security.
- Investigate existing security control frameworks that govern WLANs.
- Determine the components that should form part of a WLAN Security Control Framework to meet the needs of SMMEs in South Africa.

## 1.6 Research Process

The research process is discussed in detail in Chapter 2. The study adopted a Design Science methodology, using the inductive method to collect the information required to develop a framework. Qualitative data was collected by means of a literature review and observations. The framework was validated using a focus group.

## 1.7 Scope and Delineation of the Study

The study was limited to the security of WLANs in SMMEs in South Africa. The study focused on the design and development of a framework that SMMEs could use via a literature review and argumentation. The literature review focused on existing literature on SMMEs in South Africa, WLAN technologies and international security control framework standards.

The WLAN security control framework that was developed was then validated by means of a review by a focus group of subject experts. However, the study did not include a real world implementation of the framework developed.

## 1.8 Ethical Considerations

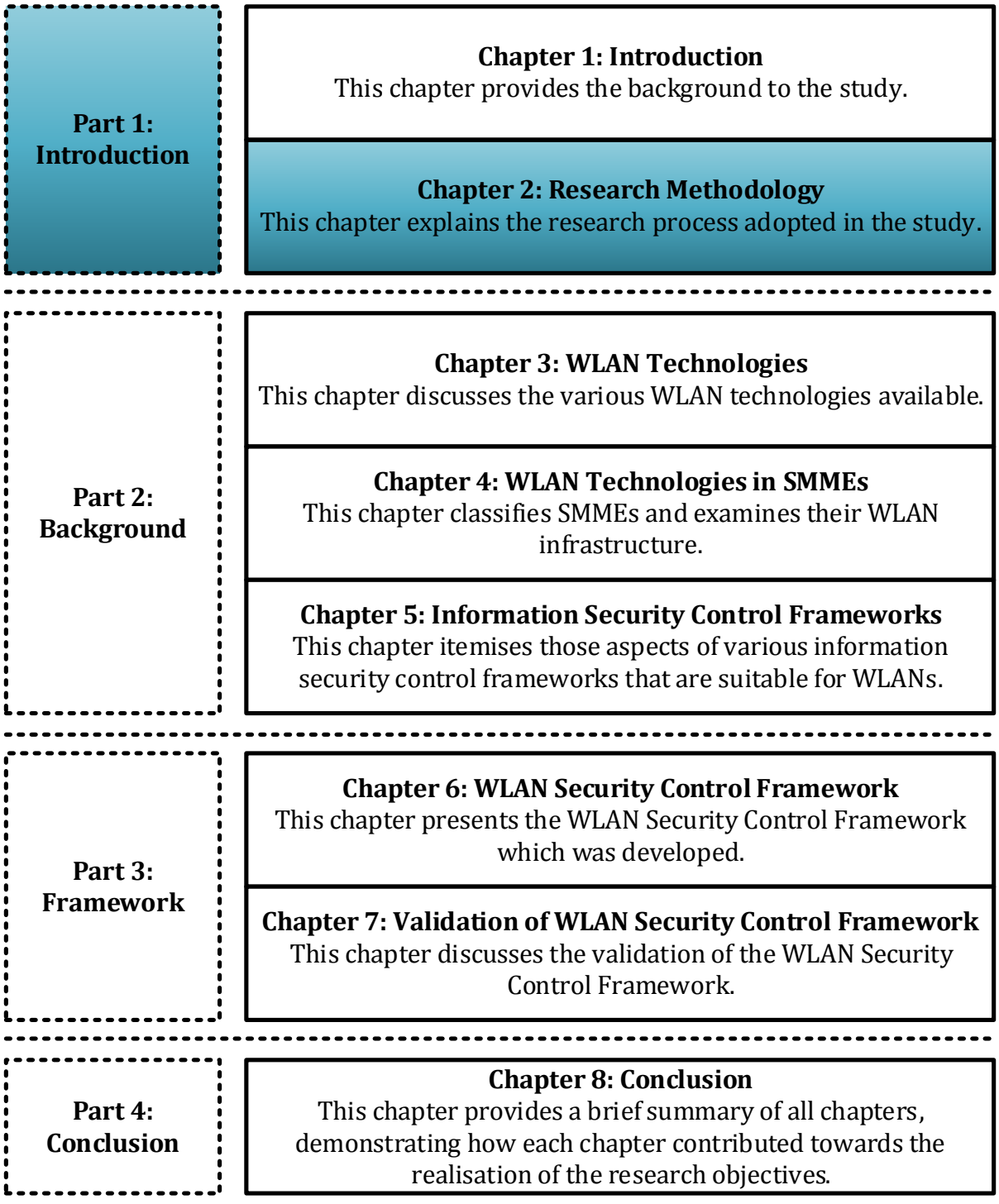
No vulnerable groups, as defined by the Nelson Mandela Metropolitan University's ethical guidelines, were involved in this research study and, thus, no further ethical consideration was required.

## 1.9 Layout of Chapters

- **Chapter 1: Introduction** – This chapter provides the background to the study.
- **Chapter 2: Research Methodology** – This chapter explains the research process adopted in the study.
- **Chapter 3: WLAN Technologies** – This chapter discusses the various WLAN technologies available.
- **Chapter 4: WLAN Technologies in SMMEs** – This chapter classifies SMMEs and examines their WLAN infrastructure.
- **Chapter 5: Information Security Control Framework** – This chapter itemises those aspects of various information security control frameworks that are suitable for WLANs.

- **Chapter 6: The WLAN Security Control Framework** – This chapter presents the WLAN Security Control Framework which was developed.
- **Chapter 7: The Validation of the WLAN Security Control Framework** – This chapter discusses the validation of the WLAN Security Control Framework.
- **Chapter 8: Conclusion** – This chapter provides a brief summary of all the chapters, demonstrating how each chapter contributed towards the realisation of the research objectives.

# 2 Research Methodology



## 2.1 Introduction

Section 2.2 presents an overview of the research methodology that was followed during the study. This overview encompasses the research philosophy, research approach, research strategy and choices, time horizons and the techniques and procedures used. The actual research process is described in section 2.3 and the chapter is concluded in section 2.4.

## 2.2 Research Methodology

The research onion as presented by Saunders, Lewis, and Thornhill (2007) is used in order to describe the research methodology adopted in the study. A summary of the methodology used for this purposes of this study is provided in Figure 2.1.

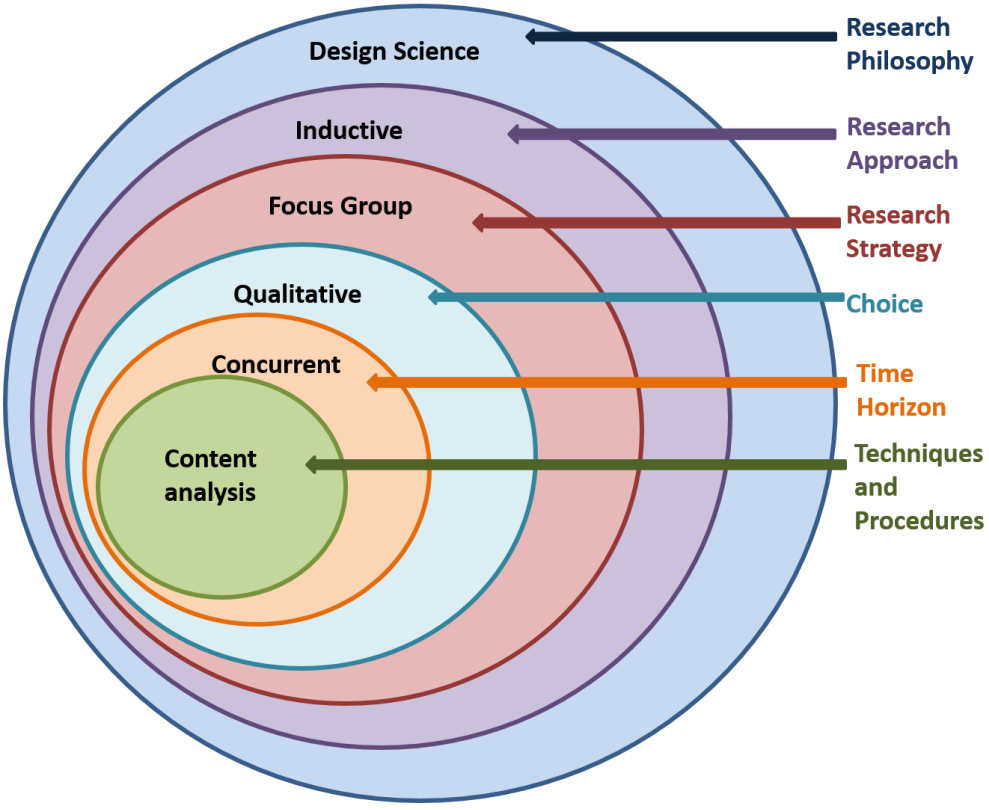



Figure 2.1: Research methodology illustrated using the research onion model (Saunders et al., 2007).

### 2.2.1 Research Philosophy

The research philosophy depends on the way in which the researcher views the world surrounding the particular research area. According to Mouton (2001), one may view this world as the world of meta-science, in which case the philosophical paradigms may be

either positivism, realism, postmodernism, critical theory, phenomenology or else the design science paradigm which is popular in the engineering field.

Research involves understanding a particular phenomenon – in the case of this study the security controls that are required for wireless local area networks (WLANs) in small, medium, and micro enterprises (SMMEs) in South Africa. Phenomenology is used when the events and issues which are being investigated are external to the individual. Thus, phenomenology refers to how the researcher is able to make sense of the world around him/her and involves either detailed suggestions about individual situations or the description of experiences. Phenomenology lends itself to qualitative research (Babbie, 2005; Leedy & Ormrod, 2001; Mason, 2002).

When following the phenomenological approach, the researcher studies a particular situation by means of interviews, observations, conversations and other inductive methods including text analysis, thereby gaining various perceptions of the situation. There are no hypotheses with which to start and the final findings are produced without the researcher having had any preconceptions or ideas about the situation in question (Lester, 1999).

There is a difference between natural science and design science (which is the more artificial of the two). As regards the particular phenomenon studied in this research study, it was possible to use design science to investigate the existing situation, namely, the securing of WLANs in SMMEs. Thus, tor the purpose of this research study **design science** was chosen as the overarching philosophical paradigm. Design science involves developing something, in this case a WLAN Security Control Framework (Vaishnavi & Kuechler, 2004).

In design science research the researcher becomes aware of a problem and develops a solution to the problem which must then be validated. The design science researcher may be a pragmatist who attempts to manipulate and control the environment (Vaishnavi & Kuechler, 2004).

The use of certain of design science guidelines, as proposed by Hevner, March, Park, and Ram (2004), made it possible to ensure that this research study had been conducted correctly – See further explanations below (Hevner et al., 2004; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007):

1. Design as an artefact – The framework that was developed in this research study was a product in itself and, thus, it served as an artefact in terms of design science.

2. Problem relevance – The relevance of the research problem was argued in section 1.3.

3. Design evaluation – The framework was developed by examining typical SMME WLAN infrastructures and identifying the WLAN security needs of the SMMEs, thereby evaluating their security level. The framework itself was presented after argumentation while the framework was validated using a focus group (see section 2.2.4).

4. Research contribution – It was anticipated that the framework developed would contribute to the securing of WLANs in SMMEs.

5. Research rigour – The study was conducted using the design science research methodology (Peffers et al., 2007), which includes defining objectives, creating an artefact, demonstrating the artefact's use, evaluating the solution to the research problem and, finally, communicating the research outcomes to relevant audiences.

6. Design as a search process – The process of building the framework was iterative and was refined after several cycles.

7. Communicate the research outcomes – The framework was communicated to relevant audiences by means of this research document and also other research papers.

### 2.2.2 Research Approach

The research approach followed may use either inductive or deductive reasoning. Inductive reasoning involves observing data and producing concepts and patterns. Thus, this implies "theory building research". On the other hand, deductive reasoning uses theory first and arrives at conclusions, thus implying "theory testing research" (Bhattacherjee, 2012; Mouton, 2001; Olivier, 2009).

This research study used **inductive** reasoning. Thus, the information required was collected and the framework developed on the basis of the information collected. Further induction was applied when the framework was validated.

### 2.2.3 Research Strategy, Choice and Data Collection

Research strategies may be categorised either as quantitative or qualitative research or a mixture of the two.

**Qualitative research** was deemed appropriate to the purposes of this particular research topic because the sources of data were primarily textual, although the data could also be collected through observation and experience. It was essential that the researcher remained objective while conducting qualitative research study (Bhattacherjee, 2012; Myers, 1997; Olivier, 2009).

The stages of the research study are depicted in Table 2.1 together with the data collection methods used in each stage.

Table 2.1: Overview of research questions with their data collection strategies

| **Research question** | **Data collection techniques** | **Source of data (qualitative)** |
|---|---|---|
| 1. *What are the needs of SMMEs with regard to WLAN security?* | Literature review, observation and experience | Literature on SMMEs<br>Literature on WLANs<br>Literature on WLAN security<br>Experience while assisting with SMME networks<br>Perceptions of SMMEs with respect to WLANs |
| 2. *Which security control framework standards govern WLANs?* | Literature review | Literature on security control framework standards |

| | | |
|---|---|---|
| 3. *What components should form part of a WLAN Security Control Framework that will be specific to the needs of SMMEs in South Africa?* | Literature review | Components from all the above sources |

For the purposes of this study qualitative data only was required. The literature reviews were necessary for this research and qualitative content analyses were also conducted. In addition, the experiences and theoretical knowledge of the researcher were taken into account. The data collected enabled the researcher to build the framework.

### 2.2.4 Methods for Validation

As stated in section 2.2.1, this study utilised design science as its research philosophy. The validation of the artefact (WLAN Security Control Framework) is part of the design science process to help ensure the rigour of a research study. Such validation may be achieved qualitatively by means of either a focus group or an expert interview. Both methods are discussed in the following sub-sections in order to provide support for the validation method adopted in this research study. Firstly, the focus group is discussed and then expert interviews.

#### *2.2.4.1 Focus Groups*

A focus group is a method used in which qualitative data is collected by engaging a small number of people in an interactive manner and focusing on a particular issue or topic. There are both advantages and disadvantages to focus groups (Carson, Gilmore, Perry, & Gronhaug, 2001; Krueger & Casey, 2000; Marshall & Rossman, 2011; Wilkinson, 2004):

The advantages of a focus group include the following:

- The focus group provides a social environment in which the participants are encouraged to share their opinions without there being any pressure to reach a consensus.
- Questions and issues may be identified which had not occurred to the researcher.

- The focus group is flexible, thus enabling the participants to explore issues as they arise.
- It is an efficient and cost-effective method for obtaining data from multiple participants.

The disadvantages of a focus group include the following:

- It may prove difficult to assemble the participants.
- It is essential that the facilitator is skilled in conducting such groups.
- The focus group does not take place in a natural setting as the participants are aware they are being observed.
- The results may be unbalanced as a result of group dynamics.
- The information obtained may either be suppressed or biased as a result of a lack of confidentiality and anonymity.

#### *2.2.4.2 Expert Interviews*

According to Marshall and Rossman (2011), an expert interview is a specialised type of interview that focuses on a particular interviewee, namely, "the expert". Expert individuals are persons who are regarded as prominent, influential and/or well informed in an organisation or community. Expert individuals are selected as participants based on their knowledge and skills in areas relevant to the research in question. Expert individuals may also be selected as a result of their distinct perspectives (Gillham, 2000). There are both advantages and disadvantages to expert interviews (Hochschild, 2009; Marshall & Rossman, 2011; Tansey, 2007).

The advantages of an expert interview include the following:

- The interviewer may triangulate between the interviewees without revealing the names of previous subjects.
- The interviewees are able to provide a general view of an organisation or its affiliates.
- The interviewees are able to provide valuable information as a result of the positions they hold in an organisation, e.g. they may report on an organisation's policies, past histories and future plans from a specific viewpoint.

The disadvantages of an expert interview include the following:

- It may be difficult to gain access to the experts in view of their time constraints.
- The interviewer may need to adapt the questions in such a manner as to enable the expert the freedom to use his/her knowledge and imagination.

Based on the above discussion on focus groups and expert interviews, it is evident that both methods could have been used to validate the WLAN Security Control Framework. However, this research study used a **focus group** method because the researcher was of the opinion that the multidisciplinary nature of a focus group would satisfy the requirement for information security knowledge, networking knowledge, and general research experience.

### 2.2.5 Time Horizons

The time horizons layer of the research onion show either a concurrent or a longitudinal study, depending on when the information is gathered. In a longitudinal study some of the measurements depend on earlier measurements and, therefore, different data is collected at a later date. In this study, much of the information gathering was conducted **concurrently**.

### 2.2.6 Techniques and Procedures

The sources of information for this research study were tabled in Table 2.1. It has also already been stated that qualitative data was gathered from these sources. The main data collection techniques used in this study included literature studies during which **content analysis** was done. Rigorous research arguments were prepared in accordance with the guidelines proposed by Mason (2002) for evidential or interpretive arguments. The framework that was developed contained concepts, theories and expectations to support and inform SMMEs about securing their WLANs. The contents of the framework were the result of the data collection techniques which were used as well as the researcher's knowledge, experiences and observation of SMMEs (Krippendorff, 2004). A focus group was used to validate the framework which had been developed.

## 2.3 Research Process

This study commenced with a research proposal which intended to show that there is a lack of WLAN security frameworks that are suitable for use by SMMEs in South Africa. Unfortunately the researcher was not able to find sufficient literature on the topic and

had to conduct a brief survey which involved 64 participants in order to demonstrate the need for such a framework.

The researcher set out to answer the first sub-question which involved identifying the needs of SMMEs with regard to WLAN security. A literature study was conducted on the topic of WLANs and, in particular, on securing WLANs in terms of physical security, technical security and operational security. SMMEs were then classified and their dependence on network infrastructure and WLANs, in particular, was examined.

The next sub-question necessitated a literature study on the security control framework standards that govern WLANs. The researcher identified three control frameworks that were then studied in detail, namely, Control Objectives for Information and Related Technology 5 for Information Security (COBIT 5), the International Organisation for Standardization and the International Electro-technical Commission 27002:2005 (ISO 27002), and the Information Security Forum Standard of Good Practice 2012 (ISF SoGP). It was found that these frameworks were not entirely suitable for SMMEs as they were aimed at the larger corporations. Thus, despite the fact that they incorporated certain network security controls, these were not specifically tailored to securing WLANs.

The final sub-question involved determining the components that were suitable for a WLAN Security Control Framework that would be specific to SMME needs in South Africa. An iterative process was followed in order to develop the framework. The information technology and networking requirements of SMMEs were taken into account in order to identify appropriate controls from the three security control frameworks that were suitable for inclusion in the WLAN Security Control Framework. Certain controls were refined to render them more applicable to the WLANs of SMMEs while some new controls were also introduced.

After a number of iterations the final framework, was presented to a focus group for validation. An instrument in the form of a questionnaire was administered to the focus group to assist in the validation. The focus group was successful and the framework was deemed valid for securing the WLANs of SMMEs.

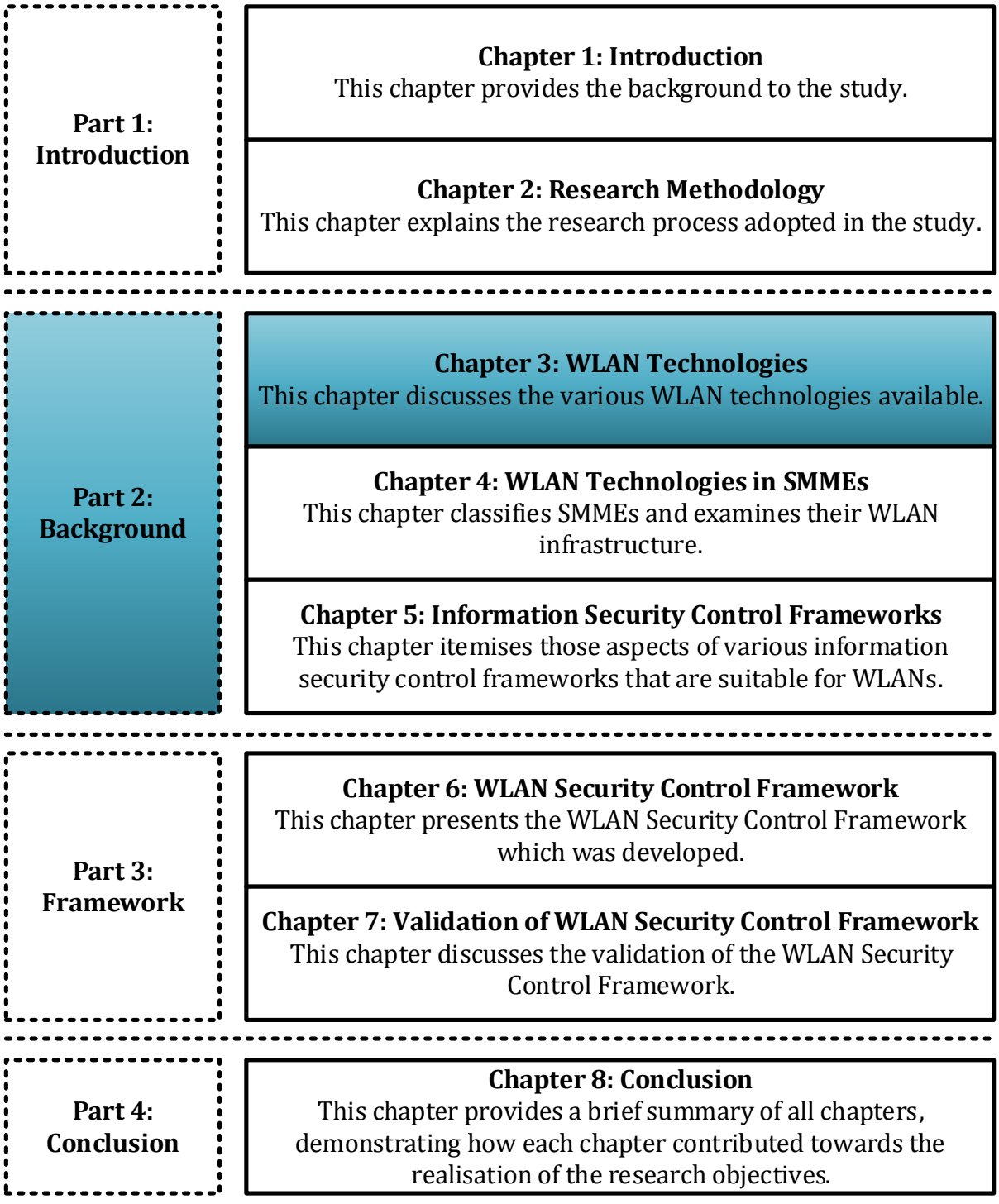
It was anticipated that the outcomes of the research study would also be presented by means of publications.

## 2.4 Conclusion

This chapter discussed the research methodology used in the study by means of the research onion as presented by Saunders et al (2007). The *research philosophy* used *was that of design science* in terms of which the researcher becomes aware of a problem and develops a solution to the problem. Design science is useful for *phenomenological philosophy*. The *research approach* involved the *inductive approach* to collecting the information required for developing a framework. The *research strategy* adopted resulted in *qualitative* data being collected by means of literature reviews, observations and experience. A *focus group* was used to validate the framework.

The literature review in the next chapter focuses on the WLAN Infrastructure of SMMEs.

# 3 WLAN Technologies



## 3.1 Introduction

Wireless local area network (WLAN) technologies have helped to simplify networking by enabling multiple end users to share resources simultaneously in either a home or a business without the need for physically connecting the devices concerned with wires.

Section 3.2 of this chapter discusses information technology networks. This is followed by a discussion of WLAN technologies in section 3.3 and specific threats that companies may face when using WLANs in section 3.4. Section 3.5.explains the security required for WLANs while section 3.6 concludes the chapter.

## 3.2 Information Technology Networks

Every business is in possession of information that is of strategic importance. In addition, the majority of businesses are required to communicate with customers, suppliers and other businesses. Information technology (IT) and networks, in particular, are important business enablers. IT networks provides a facility for borderless communication, bringing businesses closer together by removing barriers related to distance (Tapscott & Caston, 1993).

Remote programs, databases and other resources become accessible via the use of IT networking, with communication becoming faster than before and the competitive edge advancing. There are also numerous other advantages to IT networking, including reduced costs as a result of the sharing of resources and the use of networking instead of large mainframes. The ability to connect to other businesses enables flexibility and increases the availability of IT and business resources (Sanders, 2011).

However, relying on networking technologies to meet the majority of business requirements necessitates due diligence in the purchasing, implementation and maintenance of the IT networks.

There are many types of IT networks that businesses may use. Local area networks (LANs) usually comprise a group of computers which are connected together in the same building. On the other hand, the computers in wide area networks (WANs) may be further apart and connected by either telephone lines or radio waves because of the distances between the computers. There are other types of networks in between LANs and WANs, for example campus area networks (CANs) and metropolitan area networks (MANs) (Baumann, 2002).

All of these IT networks may be built using either wired or wireless technologies. This research study focuses on wireless local area networks (WLANs). The next section discusses WLAN technologies.

## 3.3 WLAN Technologies

In 1997 the Institute of Electrical and Electronic Engineers (IEEE) developed a set of required standards for implementing WLAN communication between computers and pre-existing networks, including home and office networks, and the Internet. In the decade and a half since their release, WLANs have matured and grown immensely in terms of capability, changing the face of computing and communication in the world at large. However, WLANs have also become a long, confusing list of IEEE standards, bound to the past by the required backwards compatibility (Rackley, 2011).

WLANs for the home and office networks came into being in 1999 with the release of WLAN access points that used technology based on the first two commercial WLAN standards, namely, 802.11a and 802.11b. Wired computer networking had already been standardised under the code IEEE 802 and, thus, WLAN, as a subset of computer networking, became IEEE 802.11 (Rackley, 2011).

WLANs operate in two main frequency bands which are commonly referred to as 2.4GHz and 5GHz. The main difference between the 2.4GHz WLAN and the 5GHz WLAN frequencies is signal range as the 2.4GHz frequency is able to reach farther than the 5GHz frequency. However, there is one problem with the 2.4GHz signals as they operate at the same frequency as microwave ovens and, thus, switching on a microwave oven in order to cook food degrades a 2.4GHz signal significantly (Rackley, 2011). The following sub-sections discuss the various WLAN technologies.

### 3.3.1 802.11a

The 802.11a standard, developed in 1999, uses the 5GHz frequency band and may operate at transfer speeds of up to 54Mbps. However, unless WLAN client devices have a line of sight to a WLAN 802.11a access point, the devices will not achieve such speeds. The 802.11a devices work efficiently at short distances from the WLAN access point but, at larger distances or in a large home or office, the devices may either lose signal or, even if the signal has reached the access point, the signal would be significantly diminished. Accordingly, as the range limitations of 802.11a became an issue for the widespread

adoption of WLAN devices, a second WLAN protocol was developed, namely, 802.11b (Lewis & Davis, 2004).

### 3.3.2 802.11b

The 802.11b standard, developed in 2000, uses the 2.4GHz frequency band and supports a maximum data transfer rate of 11Mbps. The slower speed of 802.11b was not a significant at the time of its development as a result of the state of the Internet as the fastest Internet connections were connecting between 4 to 6Mbps. The 802.11b worked better in the average home or office building than the 802.11a and, thus, became the standard used WLAN and the 2.4GHz frequency band was used effectively for nearly a decade (Lewis & Davis, 2004).

### 3.3.3 802.11g

In 2003, the 802.11g WLAN standard was ratified. Combining some of the algorithms used in 802.11a to achieve faster data speeds, but built upon the existing 2.4GHz 802.11b standard, the WLAN 802.11g was able to achieve the same 54Mbps speed as 802.11a, but travel the same distances as 802.11b (Eldad & Stacey, 2013).

### 3.3.4 802.11n

The 802.11n WLAN standard was made official in 2009. This standard allows for data transfer speeds of up to 300Mbps. With the introduction of this standard, WLANs could now be used to transfer larger files in a home or office network, without requiring the users to plug in via a network cable. The 802.11n WLAN standard may be used in both the 2.4GHz and the 5GHz frequency band (Eldad & Stacey, 2013) (IEEE 802.11n-2009).

### 3.3.5 802.11ac

The 802.11ac standard, ratified in 2012, was the latest WLAN standard at the time of this research study. It is the second revision of the WLAN 802.11a standard and supports transfer speeds of up to 1300Mbps. The 802.11ac WLAN standard uses the 5GHz frequency band (Eldad & Stacey, 2013).

It is clear from the discussion above that WLAN technologies have improved significantly in recent years. However, as discussed in the next section, these WLANs are vulnerable to an increasing number of threats.

## 3.4 WLAN Threats

The use of WLANs is accompanied by specific information security related responsibilities. This section will discuss the various threats that face WLANs.

When employees discover that their organisation is not deploying WLANs, they sometimes take the matter into their own hands and install their own WLAN access points, thus creating significant breaches in the corporate network security infrastructure. Accordingly, security is an important topic that merits discussion when a WLAN is implemented (Cisco Systems, 2003).

### 3.4.1 Malware Threats

The threat of malware to a WLAN is caused by malicious software which has been developed for the purpose of compromising information and harming networks. Malware threats may be targeted against either an organisation or an individual. They typically include the following (Information Security Forum, 2012):

- **Viruses/worms** – These are self-replicating programs that propagate between WLAN devices and perform one or more unauthorised actions such as corrupting information on the WLAN or transmitting an organisation's information to unauthorised individuals.
- **Trojan horses** – These are malicious programs that masquerade as authorised programs and transmit an organisation's information to unauthorised individuals.

### 3.4.2 Hacking Threats

Hacking threats to WLANs involve unauthorised external individuals deliberately attempting to access or harm an organisation's network by exploiting vulnerabilities and bypassing security controls. Hacking threats are deliberate and malicious in nature. They typically include the following (Information Security Forum, 2012):

- **Denial of service attacks** – This involve an external individual deliberately overloading systems and WLAN devices, often in order to degrade an organisation's network operations.
- **Unauthorised use of access credentials**, which involves an unauthorised user using valid credentials to gain access to a WLAN. These threats are often the result of identity theft.

- **Unauthorised WLAN scanning**, which involves an unauthorised individual probing and scanning WLAN devices to gather information that may be used to perform an attack.
- **Unauthorised tapping of WLAN traffic**, which is often referred to as "eavesdropping" and involves the interception or modification of information as it is transmitted over WLANs.
- **Unauthorised decryption of sensitive information**, which involves an unauthorised individual using techniques such as cracking passwords and brute force attacks to decrypt information over a WLAN.
- **Theft of authentication details**, which involves an unauthorised individual gaining access to an organisation's WLAN by using access control information such as passwords and encryption keys.

### 3.4.3 Social Engineering Threats

Social engineering threats involve the use of social tactics to exploit individuals and persuade them to perform specific actions such as disclosing WLAN authentication information. There are a variety of techniques that may be used including deception, manipulation and intimidation. Social engineering threats are deliberate and malicious in nature and involve activities such as blackmail, scams and threats. They typically include the following (Information Security Forum, 2012):

- **Impersonation**, which involves an unauthorised individual pretending to be another person in order to gain information on how to access an organisation's WLAN.
- **Phishing**, which is a method that uses communication channels such as emails and websites that appear to be legitimate in order to mislead recipients into divulging sensitive WLAN information.

### 3.4.4 Misuse Threats

Misuse involves the unauthorised use of resources and privileges to gain access to information on a WLAN. Misuse threats are deliberate and may be either malicious or non-malicious in nature. They typically include the following (Information Security Forum, 2012):

- **Unauthorised modification of user access**, which involves granting a user administrative access to a WLAN without approval or sign-off by management. This may, in turn, lead to administrative abuse.
- **Unauthorised system activity**, which involves users using the WLAN to carry out unauthorised activities such as downloading movies and music. These activities place a strain on the WLAN network performance.

### 3.4.5 Physical Threats

Physical threats are typically associated with the loss or theft of WLAN equipment. Physical threats may be deliberate acts of theft, tampering or sabotage, or negligence on the part of an individual. They typically include the following (Information Security Forum, 2012):

- **Unauthorised physical access**, which involves unauthorised individuals deliberately gaining access to the locations which house the WLAN equipment by either tailgating or pretending to be an authorised individual.
- **Theft or loss of WLAN equipment**, which can happen either on an organisation's premises or off-site. The WLAN equipment may include access points, laptops, cell phones and tablets.

### 3.4.6 Error Threats

Error threats to WLANs are usually the result of mistakes made by one or more individuals. Such mistakes may be the result of an unintentional action, such as the misconfiguration of a WLAN device or the malfunction of the hardware. Error threats are linked to weaknesses that involve either the human element or the hardware. They typically include the following (Information Security Forum, 2012):

- **User errors**, which are mistakes made by staff members using WLANs such as connecting to incorrect service set identifiers (SSIDs).
- **Technical errors**, which are mistakes made by information technology (IT) administrators when configuring or deploying WLANs.
- **System overload**, which is excessive WLAN activity, thus causing WLAN performance degradation or failure.
- **WLAN equipment malfunction**, which refers to the failure of WLAN hardware.

### 3.4.7 Environmental Threats

Environmental threats are typically associated with WLANs being affected by either natural events, such as floods or storms, or man-made events, such as fires, explosions, riots or electrical interference. Environmental threats may be either accidental or intentional. They typically include the following (Information Security Forum, 2012):

- **Natural disasters**, which include storms, fires and flooding and they all may have a negative effect on WLANs.
- **Accidental physical damage**, which involves the unintentional material damage of WLAN equipment. Such material damage usually affects the functioning of WLAN equipment.
- **Malicious physical damage**, which involves deliberate, material damage to WLAN equipment such as electrical interference or fire. Such material damage usually affects the functioning of WLAN equipment.
- **Power failure**, which refers to the loss of power to WLAN equipment, thus resulting in a loss of functionality.
- **Malicious jamming of WLAN**, which impedes wireless communications from reaching the intended recipients.

It is necessary to counteract all the threats that have been mentioned above by implementing appropriate security controls. The next section discusses WLAN security.

## 3.5 WLAN Security

The importance of WLAN security is increasing every day. The news is filled with reports of data breaches with customer data being lost and companies being forced to manage the crises. The threats listed in the previous section may cause substantial financial losses to organisations. Thus, instead of waiting for security incidents to occur and then respond, it is essential that organisations proactively secure their WLANs (Wong & Yeung, 2009).

The three main goals of WLAN security are to protect an organisation from the loss of confidentiality, the loss of integrity and the loss of availability. Most security practices and controls are based on protecting an organisation against losses in one or more of these areas. These areas are often referred to as the CIA triad and they comprise the core principles of information security (ISO/IEC 27002, 2005):

- Confidentiality ensures that WLAN data is not disclosed to unauthorised users.
- Integrity ensures that WLAN data is both correct and current.
- Availability ensures that WLAN devices and data are available when needed.

Organisations should be aware that any flaws in the controls designed to mitigate the loss of CIA may be exploited for malicious purposes and, thus, when organisations secure their WLANs, it is essential that they consider three different types of security, namely, physical security, technical security and operational security (Wong & Yeung, 2009).

### 3.5.1 Physical Security

Physical security is a critical element of an overall security programme. Without physical security all the other security controls and safeguards may be rendered useless. The lack of physical boundaries in WLANs creates major security issues for organisations. It is not easy to control the signal range of the WLANs and, therefore, it is highly possible that the signal will extend past the boundaries created by the wired LANs. WLANs have the potential to provide access to any user within the coverage area, even if that user is not within the organisation's physical security perimeter. Accordingly, when an organisation wishes to physically secure its WLAN, the organisation should consider the following (Bhargava & Sichitiu, 2005):

- **WLAN access point location and fixing** – Organisations should make sure that the placement of the WLAN access points allow for the desired coverage while also ensuring that there is a minimal likelihood of displacement, tampering or unauthorised removal of such points. All the WLANs risk a collapse if too many access points are out of commission, including the most important areas where employees use the wireless for work purposes.
- **Tie downs, camouflage and restricted access** – All of the WLAN access points should be physically secured by measures such as tie-down straps and camouflaging the devices. Camouflaged and secreted devices have the advantage of being hidden from the general view. Devices that cannot be seen are less likely to be compromised. Accordingly, placing access points in suspended ceilings, wiring closets or fixtures such as ornaments or pot plants improves the security of the organisation.

- **Network monitoring and site surveys** – Organisations should use tools to conduct surveys and conduct site monitoring to check for signal leakage and physical interference indicators. These tools may be used to test whether the wireless access covers all the areas that the organisation wishes to be covered while maintaining either zero leakage or as close to zero as possible. The use of bidirectional antennas may help to reduce the risk of a network being exposed to unauthorised individuals. Some organisations make use of signal jamming technologies to ensure that any leakage is rendered useless. This, in turn, helps to eliminate the risk of war driving which uses wireless scanning software with portable devices such as laptops and personal digital assistants (PDAs) to plot the wireless networks within a region.

Various devices such as cell phones, laptops and PDAs may be wireless enabled. The securing of such devices will also form part of the physical layer of security. If such devices are left unattended this may result in their being stolen, thus giving an unauthorised individual access to the organisation's entire network (Levy, Tran, Lydon, Pollock, Parry, & Weigand, 2008).

### 3.5.2 Technical Security

The technical security of WLANs is extremely important. An WLAN that has not been secured allows anyone within the wireless range access to an organisation's file servers, databases, email servers, etc. Therefore, in order to secure a WLAN properly, it is imperative that the following technical controls are implemented (Levy et al., 2008):

- **Ethernet Multiple Access Control (MAC) address filtering** – Each network interface has a unique MAC address. Configuring the WLAN access point with a MAC address which only allows authorised network interfaces to access the WLAN. Thus, any intruders attempting to gain access from their own unauthorised devices will be blocked.
- **Service set identifiers (SSID)** – The SSID acts as an identifier for a particular WLAN. It has two modes of operation, namely, open and closed. If the mode of operation is open, then the SSID of the WLAN access point is broadcast to the world whereas, if the mode of operation is closed, the SSID is hidden from the world. The benefit of a closed SSID is that the access points do not respond to

messages unless the client has the correct SSID in the message header. It is, therefore, recommended that any organisation intending to increase its security should set the SSID to closed mode as well as effect a change from the default SSID.

- **Wi-Fi Protected Access (WPA2)** – The use of the WPA2 wireless security standard means that an organisation experiences improved security connections as a result of the use of strong encryption methods. WPA2 has proved to be a secure standard when used with strong passwords in Pre-Shared Keys (PSK) or with an external authentication server using Extensible Authentication Protocol (EAP).
- **Use 802.1x to authenticate all Devices** – A rogue access point is a WLAN access point that has been created to allow a hacker to conduct man-in-the-middle attacks. The best method for dealing with the threat of rogue access points is to use 802.1x as this prevents all unauthorised devices from connecting to the network by using strong authentication methods when a device attempts to connect to a network.
- **Use of Encryption** – Encrypting all traffic over a wireless network is one of the most effective ways in which to secure a WLAN. Thus, organisations should ensure that the WLAN access point that they purchase has a built-in encryption mechanism.
- **Virtual Private Networks (VPN)** – Many organisations already have a VPN for accessing internal resources over the Internet. This same VPN may be used to give authorised users access to applications over the hostile wireless network. This, in turn, solves both the authentication and confidentiality issues of WLANs.
- **Enable logging** – Organisations should enable event monitoring and logging on all the devices in the network. These logs indicate to supply network administrators that unauthorised security-related activities have either been attempted or performed on the network. When properly designed and implemented, event logging and monitoring may assist organisations to determine what has been recorded on their systems so that there may be a follow-up investigation conducted, with remediation where necessary.

### 3.5.3 Operational Security

Physical security and technical security provide a foundation only for defining what organisations should be using in order to secure their WLANs but they do not provide a method for governing these WLAN security systems. In order to do that an organisation must draw up WLAN security policies. A WLAN security policy is a set of rules that help to govern the behaviour of employees as well as the constraints applied to and enforced by the system so as to guarantee a predefined level of security. Everything in the WLAN should be accounted for in the WLAN security policy or else there will be no WLAN security (Wong & Yeung, 2009).

It is essential that the policy cover all the obvious security threats as well as the more subtle threats. Even if the organisation's network has the highest security protection from the outside world (i.e. Internet) but it is wide open to someone tampering with it if he/she is physically on site, then this is probably in violation of the intended security policy (Information Security Forum, 2012).

The WLAN security policy should include which users may access what and which users may be given security services such as anti-virus, anti-spam, data backups and intrusion prevention. The policy should also take into account the location and security of the organisation's endpoints and where employees are allowed to access the WLAN (Information Security Forum, 2012).

In addition, the WLAN security policy should include processes that enable the organisation to handle unexpected events, including procedures for data protection and disaster recovery as well as user account lifespans and termination protocols (Information Security Forum, 2012).

Finally, a WLAN security policy must include a process to ensure all systems are current and ready to carry out the core elements of the policy. This includes version updates for clients, servers and network devices and training users and staff on how to use the equipment in a safe and secure way (Baumann, 2002).

Formulating a WLAN security policy is an intricate process. It would, therefore, be highly beneficial to an organisation to hire an expert security consultant to go over the WLAN security policy. The best way of uncovering loopholes in a WLAN security policy is to have as many people as possible go over it (Levy, et al., 2008).

Once an organisation has formulated the WLAN security policies the organisation must devise the procedures for the way in which the policies will be carried out. Such procedures are the operational processes which are required in order to implement the policies (Levy, et al., 2008).

The procedures may include the following:

- The steps taken to configure the WLAN security on the devices.
- How users access the WLANs, including the applications to use.

An effective security education, training and awareness programme will explain the actual rules and expected behaviour to the employees in an organisation. It is essential that such programmes communicate the policies and procedures that need to be followed so that employees may be held accountable if they are negligent (Wilson & Hash, n.d.).

- Awareness programmes are designed to change behaviour and to reinforce sound security practices. The purpose of such awareness programmes is to focus employees' attention on security.
- Training strives to produce the relevant and necessary security skills and competencies. It teaches employees how to perform specific functions.
- Education integrates all of the security skills and competencies that organisations require in order need to produce WLAN security specialists and professionals who are capable of both vision and proactive response.

Once the security policies and procedures have been implemented, it is essential that processes are put in place in order to monitor compliance and effectiveness. Organisations should, thus, design automated tracking systems to capture key information regarding WLAN activity (e.g. user logons, services accessed, and usage statistics). This data should be captured in such a way so that it provides the organisation with an analysis of its awareness, training and education programmes (ISO/IEC 27002, 2005).

## 3.6 Conclusion

This chapter commenced with a brief discussion of IT networks. This was followed by a detailed discussion on WLAN technologies as well as the typical threats facing WLANs as a result of the fact that WLANs have different requirements for security as compared to

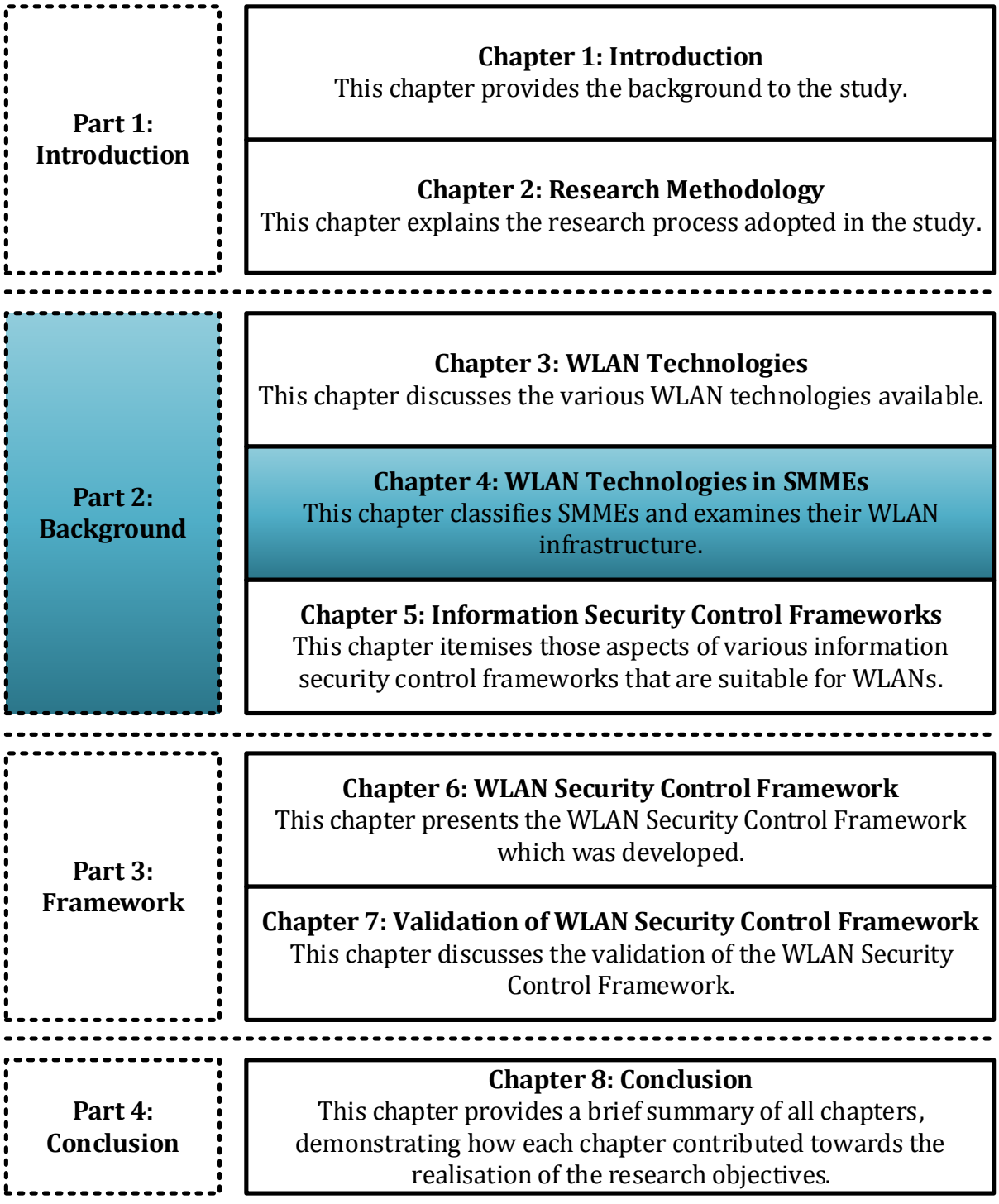
wired networks. The security controls which may be implemented to mitigate these threats were discussed in terms of physical, technical and operational security.

The cost of installing and maintaining a WLAN is, on average, lower than the cost of installing and maintaining a traditional wired LAN. The reason for this is that WLANs eliminate the direct costs of the cabling and labour associated with installation and repair. In addition, it is relatively simple both to move and to change WLANs and this, in turn, reduces the ongoing administrative costs.

Thus, WLANs open up networking possibilities for companies that are not able to afford expensive wired networking infrastructures. In view of the fact that WLANs play such a significant role in business, this research study will investigate WLANs in small, medium and micro enterprises (SMMEs).

The next chapter discusses the WLAN technologies which are suited to SMMEs.

# 4 WLAN Technologies in SMMEs



## 4.1 Introduction

It is estimated that small, medium and micro size enterprises (SMMEs) make up 91% of businesses in South Africa, while they account for between 52 and 57% of South Africa's gross domestic product (Abor & Quartey, 2010). Thus, SMMEs comprise a substantial portion of South Africa's economy and should therefore be protected appropriately to ensure their sustainability.

Section 4.2 of this chapter contains a classification of SMMEs. This is followed by a discussion on the way in which information technology (IT) and network infrastructures are enablers for SMMEs and a brief explanation of the wireless local area networks (WLANs) used by SMMEs.

## 4.2 Classifying SMMEs

Countries tend to classify businesses differently according to size. This section discusses the classifications used in three different regions, namely, the United States, European Union and South Africa as well the way in which researchers classify businesses in their research documents.

The United States (US) Small Business Act of 1953 defines a small business as "one that is independently owned and operated and is not dominant in its field of operation". In the US, the term small and medium business (SMB) is often used. The SMBs differ according to the industry in question. However, in the main, the United States identifies a small business as a business which employs fewer than 100 employees while a medium sized business refers to a business which employs between 100 and 500 employees (Small Business Administration, 2011).

The European Union (EU) uses the abbreviation SME to describe the small to medium enterprises. The current definition used in the EU categorises companies which employ fewer than 10 employees as micro enterprises, companies which employ between 10 and 50 employees as small enterprises and companies which employ between 50 and 250 members as medium enterprises. In addition, these companies may not have an annual turnover exceeding 50 million euros and/or an annual balance sheet total exceeding 43 million euros (European Commission, 2003).

The majority of researchers classify businesses according to their number of full-time employees or to their annual turnover. For example, Tapia, Correa and Manzanares

(2009), define a medium enterprise as employing between 50 and 250 employees, a small enterprise as employing between 10 and 50 employees and a micro enterprise as employing fewer than 10 employees. However, some researchers define a business according to the way in which it is controlled and owned. Fuller (2003) maintains "a small business means one that is owned by the people running it and which is relatively powerless with respect to national or global market".

The South African National Small Business Act, 1996 (South Africa, 1996) defines a small business as "a separate and distinct entity, including co-operative enterprises and non-governmental organisations, managed by one owner or more which, including its branches or subsidiaries, if any, is predominantly carried on in a sector or subsector of the economy mentioned in column 1 of the Schedule and which can be classified as a micro-, a very small, a small or a medium enterprise by satisfying the criteria mentioned in columns 3, 4 and 5 of the Schedule opposite the smallest relevant size or class as mentioned in column 2 of the Schedule". The schedule referred to in this definition has since been updated (Table 4.1) in the National Small Business Amendment Act of 2003.

Table 4.1: Extract of Schedule of the National Small Business Amendment Act of 2003 (Redrawn from Schedule of the National Small Business Amendment Act of 2003 by South Africa, 2003, Retrieved June 6, 2011 from http://www.info.gov.za/acts/1996/a102-96.pdf)

| **Column 1** | **Column 2** | **Column 3** | **Column 4** | **Column 5** |
|---|---|---|---|---|
| **Sector or subsector in accordance with the Standard Industrial Classification** | **Size of class** | **The total full-time equivalent of paid employees** | **Total turnover** | **Total gross asset value (fixed property excluded)** |
| Agriculture | Medium | 100 | R5 m | R5 m |
| | Small | 50 | R3 m | R3 m |
| | Very Small | 10 | R0.50 m | R0.50 m |

| | | | | |
|---|---|---|---|---|
| | Micro | 5 | R0.20 m | R0.20 m |
| Mining and Quarrying | Medium | 200 | R39 m | R23 m |
| | Small | 50 | R10 m | R6 m |
| | Very Small | 20 | R4 m | R2 m |
| | Micro | 5 | R0.20 m | R0.10 m |

As shown in Table 4.1, the classification of the size of a business depends on several factors. These factors include the sector or subsector in accordance with the Standard Industrial Classification, the total full-time equivalent of paid employees, the total turnover and the total gross asset value of the business (South Africa, 2003). In South Africa such businesses are referred to as SMMEs.

It is clear from the discussion above there are many different classifications for SMMEs. This research study uses a generic classification method as depicted in Table 4.2. As may be seen in the table, micro-sized enterprises employ between one and five employees, small-sized enterprises between six and 50 employees and medium-sized enterprises between 51 and 200 employees. **Enterprises with more than 200 employees are regarded as large enterprises and are not be included in the scope of this study**.

Table 4.2: Enterprise classifications used for the purposes of this study.

| Size of class | The total full-time employees |
|---|---|
| **Micro enterprises** | 1–5 employees |
| **Small enterprises** | 6–50 |
| **Medium enterprises** | 51–200 |
| **Large enterprises** | More than 200 |

## 4.3 IT as an Enabler in SMMEs

Information technology has enabled SMMEs to connect with other parties throughout the world using powerful tools such as email or the Internet, thus making it possible for them to reach broader markets than would otherwise be the case. Communication tools such as cell phones or smartphones have resulted in numerous improvements for both the employees and the customers of SMMEs. Text messaging and social networks have also facilitated communication. In addition, SMMEs are able to market and advertise in order to reach new customers using search engines and online advertising. Productivity has improved because it is possible to complete tasks more quickly by using technology. The SMMEs and their customers have been brought closer together with this resulting in improved customer service. SMMEs are now able to provide telecommuting and flexi time benefits by using email, online collaboration tools and mobile computing while SMMEs are also able to extend their reach by using teleconferencing to include global customers and employees (Mitra, 2005).

Thus, IT has become a key tool which management is able to use in order to ensure operational benefits and to grow the business. All the strategic initiatives behind a transaction are heavily reliant on IT and, thus, it is no longer possible for businesses either to ignore IT or to view it merely as a back-office function if they want to achieve growth. Like the larger corporations, SMMEs also make use of IT and networking, in particular, to perform the everyday business functions. The next section discusses the appropriate networking infrastructure for SMMEs (Overby, Bharadwaj, & Sambamurthy, 2006).

## 4.4 SMME Networking Infrastructure

Networking infrastructures facilitate the IT communication required for business. A network infrastructure is an interconnected group of computer systems which are linked by various components of the telecommunications architecture. These networks may operate over wired or wireless local area network (WLAN) connections or a combination of both (Sanders, 2011).

The network infrastructure includes both the physical hardware used to transmit data electronically, for example, routers, switches, gateways, bridges, cables, WLAN access points and backbones and also the software, for example, network protocols, security

controls and network access methodologies. The network infrastructures may be either open or closed, for example, the open architecture of the Internet or the closed architecture of a private local area network (LAN).

The majority of SMMEs use the simplest form of a network infrastructure. This typically consists of one or more computers, a network or Internet connection, and a device linking all the computers and systems to each another. These networks communicate with outside networks (e.g. Internet) by means of a router which bridges the networks and provides a common language for data exchange according to the rules of each network (Wong & Yeung, 2009).

When multiple computers in an SMME share an Internet connection this is considered a network infrastructure. The Internet itself is an advanced network infrastructure which serves millions of businesses, allowing them to access the global network which stores information on various systems. SMME intranets are similar to the global Internet but they operate in a closed network infrastructure which is accessible only to those within it. SMME intranets generally include the central data storage where one or more servers are located and employees are able to access the information on these servers from their individual workstations (Wong & Yeung, 2009).

## 4.5 WLANs in SMMEs

In the past WLANs were regarded as a slow and unreliable network standard (Chen, Katsaros, Nanopoulos, & Manolopoulos, 2005). The 802.11g standard, which was ratified in 2003, is now regarded as inadequate because applications have become more complex and require more bandwidth than before. The 802.11g standard struggled to stream video data efficiently because of the speeds that it offered.

The new 802.11ac standard, which was ratified in 2012, uses newer technologies and has tweaked the existing technologies to give WLANs more speed and range than was previously the case. The speed which is obtainable when using 802.11ac is up to 1300Mbps, thus making WLANs a sustainable choice for SMMEs. The various WLAN technologies are discussed in more detail in Chapter 3 (Eldad & Stacey, 2013).

The benefits of using WLANs in SMMEs include the following (Chandra et al., 2009):

- Mobility – WLAN users have the ability to access shared resources without needing a place anywhere in the organisation to plug into. A WLAN allows users to be truly mobile as long as the WLAN device is within the network coverage area.
- Range of coverage – The range of a typical WLAN access point is approximately 100 metres. WLAN access points may extend the cover of an area in such a way that the range of coverage of the access points overlap, thus providing roaming. This, in turn, enables the WLAN user to wander around and move from the coverage area of one access point to another while maintaining seamless connection within the network.
- Ease of use – WLANs are easy to use and the users require minimum experience only to take advantage of WLANs.
- Flexibility – The installation of a WLAN infrastructure can be fast and easy and may eliminate the need to pull cable through walls and ceilings. Thus, WLANs may be set up where it is impossible to install wires.
- Scalability – WLANs can be designed to be either extremely simple or extremely complex. They are able to support large numbers of WLAN devices and cover large physical areas by adding access points in order to extend coverage.
- Cost – The cost of installing and maintaining a WLAN is, on average, lower than the cost of installing and maintaining a traditional wired LAN. The reason for this is that WLANs eliminate the direct costs of the cabling and labour associated with installation and repair. In addition, it is relatively easy to move and change WLANs and this, in turn, reduces the ongoing administrative costs.

WLANs enable users to access the peripherals within wireless reach such as servers, printers and other network resources, regardless of their location. Thus, this means that the user has the ability to stay connected while working anywhere in the company – from the meeting room to the cafeteria. SMMEs have recognised the benefits of such flexibility and have deployed WLANs in high numbers. According to the 2003 Wireless LAN Benefits Study (Cisco Systems, 2003), WLAN users stay connected to a corporate network for 3.5 hours per day longer than their wired peers, thus making employees 27 percent more productive than they would otherwise have been.

When comparing the benefits of WLANs for an SMME against the total cost of ownership (TCO), it becomes clear that the use of WLANs may bring more value to a business, provided that the WLAN is secured and managed properly (Cisco Systems, 2003).

The securing and management of WLANs are, thus, extremely important and require considerable, attention especially in view of the fact that WLANs tend to be exposed to more threats than wired networks.

SMMEs, in particular, do not usually have on-site security support personnel and may not have funds required to outsource the WLAN security functions. This, in turn, often implies a lack of the required knowledge, skills and resources as regards securing WLANs on the part of SMMEs.

It would, therefore be extremely useful for SMMEs to have access to guidelines derived from accepted international information security control frameworks and standards and to use these in their own in-house implementation and securing of their WLANs.

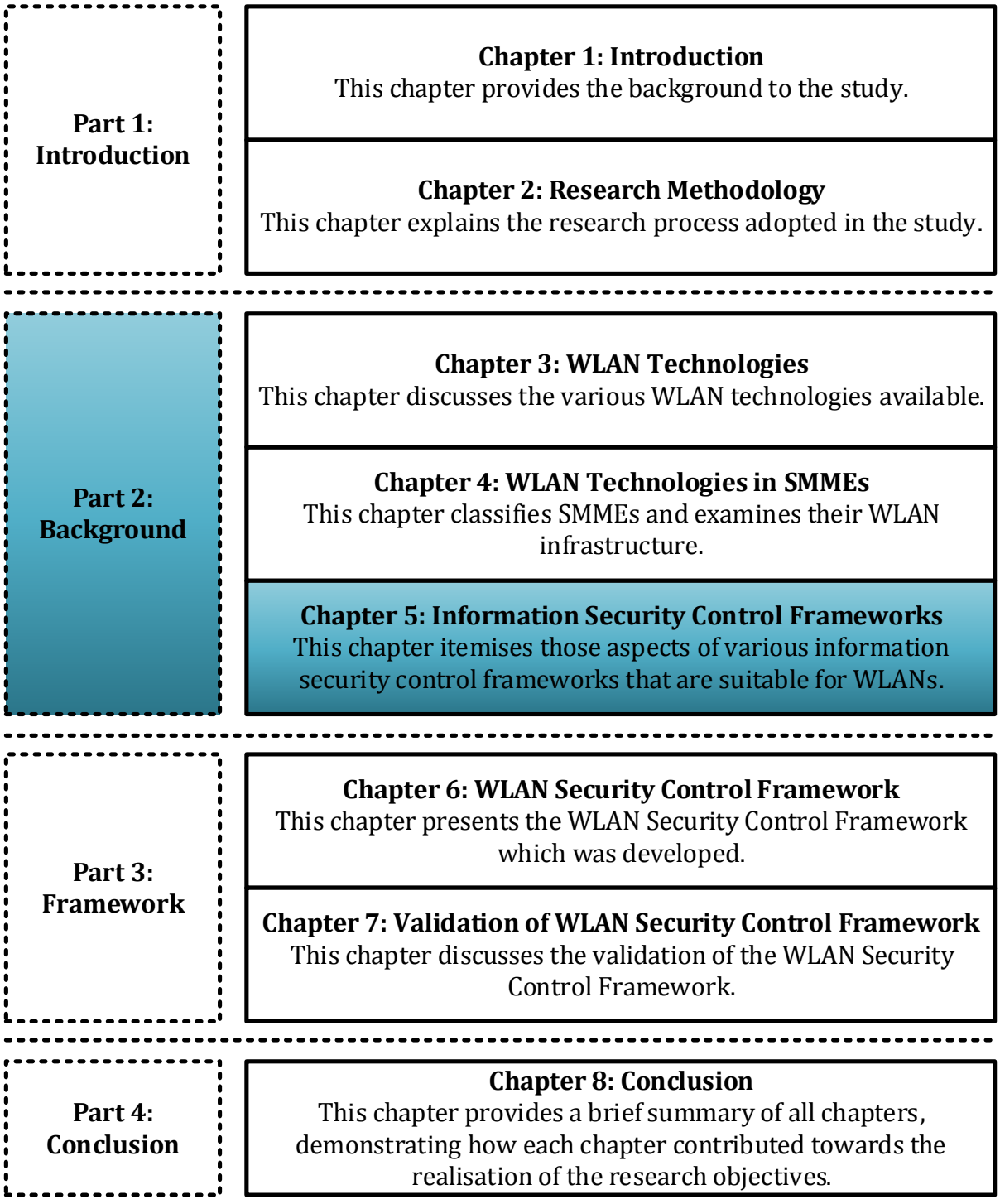
## 4.6 Conclusion

This chapter discussed WLANs in the context of SMMEs and their needs. The chapter started by classifying SMMEs and proceeded to discuss the benefits of WLANs for SMMEs.

The same WLAN security threats which were discussed in Chapter 3 as affecting larger organisations also affect SMMEs. It was also stated in Chapter 4 that WLANs are more suited to SMMEs as compared to wired networks. However, it was also seen that, in general, SMMEs do not have at their disposal the resources, knowledge, and skills required to secure WLANs effectively and, thus, WLANs often present more risks in SMME's than in larger organisations.

There is a definite need for SMMEs to have in place effective WLAN security controls. Accordingly, the next chapter will examine information security control frameworks in order to ascertain whether they meet the needs involved in securing WLANs in SMMEs.

# 5 Information Security Control Frameworks



## 5.1 Introduction

If an implementation is to be conducted in the correct manner and ensure effectiveness, it is useful to have a benchmark that has been developed using international best practices. With regard to information security there are several security control framework standards which are recognised internationally as useful guidelines for the effective implementation of information security in organisations. The use of a recognised information security framework makes it is possible to ensure the confidentiality, integrity and availability of all the information technology (IT) assets in an organisation.

This chapter will discuss various information security (IS) control framework standards, detailing how they are used and for what. Section 5.2 discusses various control frameworks and section 5.3 explains why the frameworks are aimed at the larger organisations. Section 5.4 concludes the chapter.

## 5.2 IS Control Frameworks

A control framework is a "structured way of categorising controls to ensure the whole spectrum of a control is covered adequately" (ISACA, 2012). A number of information security control frameworks have been developed to assist organisations in the securing their information assets. These frameworks include Control Objectives for Information and Related Technology (COBIT) 5 for Information Security (ISACA, 2012), International Organisation for Standardisation and the International Electro-Technical Commission (ISO/IEC) 27002:2005 (ISO/IEC 27002, 2005), Information Security Forum (ISF) Standard of Good Practice 2012 (Information Security Forum, 2012), Information Technology Infrastructure Library (ITIL) (Von Bon, 2007) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100 (NIST, 2006).

The information security control frameworks listed above all have implications for the objectives of this research study. However, in view of the magnitude of any research endeavour involved in analysing each framework three only were selected for the purposes of the this study. The control frameworks selected were COBIT 5 for Information Security, ISO/IEC 27002 and ISF Standard of Good Practice. The COBIT 5 framework was selected because it is the only framework for the governance and management of business and IT, while the ISO/IEC 27002 was selected because it

provides detailed guidelines for information security practices and is widely used amongst organisations. The ISF Standard of Good Practice was selected because the body that created it is regarded as the world's leading authority on information security and the ISF group is made up of thousands of information security specialists worldwide.

These frameworks, which were used in this research study, are discussed in the sub-sections below.

### 5.2.1 COBIT 5 for Information Security

COBIT is a framework which was created by the Information Systems Audit and Control Association (ISACA) for information technology management and IT governance (ISACA, 2012). It is a supporting toolset that enables managers to bridge the gap between control requirements, technical issues and business risks. ISACA first released COBIT in 1996. However, the version discussed in this research study, COBIT 5, was released in 2012.

*COBIT 5 for Information Security* builds on the *COBIT 5* framework in that it provides a more detailed and practical approach to information security than the *COBIT 5* framework. *COBIT 5 for Information Security* is intended for all stakeholders in the information security within an organisation, including chief information security officers, information security managers, and other information security professionals.

*COBIT 5 for Information Security* comprises a total of thirty-seven processes. As listed in Table 5.1 these thirty-seven processes are grouped into the five domains (ISACA, 2012):

Table 5.1: COBIT 5 for information security domains and processes

| COBIT 5 DOMAINS | COBIT 5 PROCESSES |
|---|---|
| **Evaluate, Direct and Monitor (EDM)** | EDM addresses a set of interactions between governance and management and is intended to result in an efficient and effective governance system. The processes in this domain include the following:<br>EDM01: Ensure Governance Framework Setting and Maintenance<br>EDM02: Ensure Benefits Delivery |

| COBIT 5 DOMAINS | COBIT 5 PROCESSES |
|---|---|
| | EDM03: Ensure Risk Optimisation<br>EDM04: Ensure Resource Optimisation<br>EDM05: Ensure Stakeholder Transparency |
| **Align, Plan and Organise (APO)** | APO addresses the strategies and tactics to be adopted and how to identify the best way in which IT may contribute to realising the business objectives of an organisation. The processes in this domain include the following:<br>APO01: Manage the IT Management Framework<br>APO02: Manage Strategy<br>APO03: Manage Enterprise Architecture<br>APO04: Manage Innovation<br>APO05: Manage Portfolio<br>APO06: Manage Budget and Costs<br>APO07: Manage Human Resources<br>APO08: Manage Relationships<br>APO09: Manage Service Agreements<br>APO10: Manage Suppliers<br>APO11: Manage Quality<br>APO12: Manage Risk<br>APO13: Manage Security |
| **Build, Acquire and Implement (BAI)** | The realisation of the IT strategy requires the identification, development and acquisition of IT solutions as well as the implementation of these solutions |

| COBIT 5 DOMAINS | COBIT 5 PROCESSES |
|---|---|
| | and their integration with the business process. The processes in the BAI domain include the following:<br>BAI01: Manage Programmes and Projects<br>BAI02: Manage Requirements Definition<br>BAI03: Manage Solutions Identification and Build<br>BAI04: Manage Availability and Capacity<br>BAI05: Manage Organisational Change Enablement<br>BAI06: Manage Changes<br>BAI07: Manage Change Acceptance and Transitioning<br>BAI08: Manage Knowledge<br>BAI09: Manage Assets<br>BAI10: Manage Configurations |
| **Deliver, Service and Support (DSS)** | DSS addresses the delivery of the required services, ranging from traditional operations in respect of security and continuity to training. Included in this domain is the processing of data by application systems which fall under application controls. The processes in this domain include the following:<br>DSS01: Manage Operations<br>DSS02: Manage Service Requests and Incidents<br>DSS03: Manage Problems<br>DSS04: Manage Continuity<br>DSS05: Manage Security Services<br>DSS06: Manage Business Process Controls |

| COBIT 5 DOMAINS | COBIT 5 PROCESSES |
|---|---|
| **Monitor, Evaluate and Assess (MEA)** | MEA addresses the regular assessment of IT processes over time as regards quality and compliance with control requirements. It also addresses performance management, monitoring of internal control, regulatory compliance and governance. The processes in this domain include the following:<br>MEA01: Monitor, Evaluate and Assess Performance and Conformance<br>MEA02: Monitor, Evaluate and Assess the System of Internal Control<br>MEA03: Monitor, Evaluate and Assess Compliance with External Requirements |

*COBIT 5 for Information* Security integrates both the business and the IT functional responsibilities and provides a clear distinction between the roles and practices of information security governance and information security management. In addition, it outlines responsibilities at various levels of the enterprise, encompassing all process steps from the beginning to the end (ISACA, 2012).

### 5.2.2 ISO/IEC 27002:2005

*ISO/IEC 27002:2005* (hereafter "*ISO 27002*") is an information security standard published by the ISO and by the IEC, and entitled *Information Technology – Security techniques – Code of practice for information security management* (ISO/IEC 27002, 2005).

*ISO 27002* contains best practice recommendations on information security management for use by those responsible for implementing information security within an organisation. *ISO 27002* best practices are intended for the stakeholders in the information security within an organisation, including the chief information security officer, information security manager and security engineers.

The *ISO 27002* comprises a total of eleven security control clauses (see Table 5.2):

Table 5.2: ISO 27002 Control Clauses and Description

| ISO 27002 CONTROL CLAUSES | DESCRIPTION |
|---|---|
| A.5: Security Policy | A.5 provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. |
| A.6: Organisation Information Security | A.6 ensures that a management framework is established to initiate and control the implementation of information security within the organisation and maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. |
| A.7: Asset Management | A.7 ensures that all assets are accounted for and have a nominated owner. It also ensures that information is classified to indicate the need, priorities, and expected degree of protection when handling such information. |
| A.8: Human Resources Security | A.8 ensures that employees, contractors and third party users understand their responsibilities, are equipped to support the organisational security policies, and exit an organisation or change employment in an orderly manner. |
| A.9: Physical and Environmental Security | A.9 ensures the prevention of unauthorised physical access, damage, and interference to the organisation's premises and information. |
| A.10: Communications and Operations Management | A.10 ensures the correct and secure operation of information processing facilities, the appropriate level of information security and service delivery in line with third party service delivery agreements, the minimised risk of system failures, the integrity of software and |

| ISO 27002 CONTROL CLAUSES | DESCRIPTION |
|---|---|
| | information, the protection of information in networks, and the security of electronic commerce services. |
| A.11: Access Control | A.11 ensures that access to information is controlled and unauthorised access is prohibited. |
| A.12: Information Systems Acquisition, Development and Maintenance | A.12 ensures that security is an integral aspect of the information systems and prevents errors, loss, unauthorised modification or misuse of information in applications. |
| A.13: Information Security Incident Management | A.13 ensures that the information security events and weaknesses associated with information systems are communicated in a manner which allows timely corrective action to be taken. |
| A.14: Business Continuity Management | A.14 ensures that interruptions to business activities are counteracted and protects critical business processes from the effects of major failures of information systems or disasters. |
| A.15: Compliance | A.15 ensures all breaches of any law, statutory, regulatory or contractual obligations are avoided and that security audits maximise effectiveness and minimise interferences. |

*ISO 27002* is important because it provides organisations with an international framework on which auditors rely for verification of the compliance with security mandates. The implementation of *ISO 27002* entails understanding and using its key concepts, principles and controls. The *ISO 27002* begins with the 11 sections of best practices outlined above and which address an organisation's requirements as exposed by a formal risk assessment. Each section presents information in terms of four categories: Objective (or objectives), Control (or controls) that helps to meet the

objective, Implementation Guidance, and Other Information. According to ISO/IEC, the standard "is intended as a common basis and practical guideline for developing organisational security standards and effective security management practices, and to help build confidence in inter-organisational activities." (ISO/IEC 27002, 2005).

### 5.2.3 ISF Standard of Good Practice

The Standard of Good Practice (*SoGP*) for Information Security, published by the ISF, is a business-focused, practical and comprehensive guide to identifying and managing the information security risks within an organisation (Information Security Forum, 2012).

The *ISF SoGP* is aligned with the information security requirements as set out in the ISO/IEC 27000 series of standards, and provides a wider and deeper coverage of both the ISO/IEC 27002 control topics, as well as wireless local area network (WLAN) security. The *ISF SoGP* is used by information security managers, business managers, IT managers, auditors, and IT service providers in organisations of all sizes.

The *ISF SoGP* comprises twenty-six security areas which are divided into the following four security categories (Information Security Forum, 2012):

- Security Governance (SG)
- Security Requirements (SR)
- Control Framework (CF)
- Security Monitoring and Improvement (SI)

Table 5.3 lists the four security *ISF SoGP* security categories together with the twenty-six security areas.

Table 5.3: ISF Standard of Good Practice 2012 Security Categories and Security Areas

| ISF SECURITY CATEGORIES | ISF SECURITY AREAS |
|---|---|
| SG: Security Governance | The Security Governance category discusses how to develop an information security strategy within the organisation’s governance framework and how to drive such strategy through an information security |

| ISF SECURITY CATEGORIES | ISF SECURITY AREAS |
|---|---|
| | programme. The security areas in this category include the following:<br>SG1: Security Governance Approach<br>SG2: Security Governance Components |
| SR: Security Requirements | The Security Requirements category discusses the functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an organisation. This category includes the following:<br>SR1: Information Risk Assessment<br>SR2: Compliance |
| CF: Control Framework | The Control Framework category discusses the various security controls that should be implemented. The controls are organised and categorised into different areas and includes security best practices and procedures. This category includes the following:<br>CF1: Security Policy and Organisation<br>CF2: Human Resource Security<br>CF3: Asset Management<br>CF4: Business Applications<br>CF5: Customer Access<br>CF6: Access Management<br>CF7: System Management<br>CF8: Technical Security Infrastructure<br>CF9: Network Management |

| ISF SECURITY CATEGORIES | ISF SECURITY AREAS |
|---|---|
| | CF10: Threat and Vulnerability Management<br>CF11: Incident Management<br>CF12: Local Environments<br>CF13: Desktop Applications<br>CF14: Mobile Computing<br>CF15: Electronic Communications<br>CF16: External Supplier Management<br>CF17: System Development Management<br>CF18: System Development Lifecycle<br>CF19: Physical and Environment Security<br>CF20: Business Continuity |
| SI: Security Monitoring and Improvement | The Security Monitoring and Improvement category discusses the monitoring processes and procedures in an organisation's security environment as well as the improvement of an organisation's security posture over time. The category includes the following:<br>SI1: Security Audit<br>SI2: Security Performance |

When the *ISF SoGP* is implemented comprehensively, organisations are able to build an Information Security Management System (ISMS), perform information risk assessments, and implement security controls beyond those defined in *ISO 27002*, and include topics not addressed by *ISO 27002*, such as cloud computing, cybercrime attacks and consumer devices (Information Security Forum, 2012).

## 5.3 IS Control Frameworks and Larger Organisations

It is clear from the above discussion on these information security control framework standards that they are aimed at larger organisations. For example, COBIT 5 BAI05

requires the presence of a qualified information security professional to serve on all the IT implementation teams. ISO 27002 A.6 Organisation Information Security states that information security activities should be co-ordinated by representatives with relevant expert roles and job functions. ISO 27002 A.15 Compliance indicates that a specific data protection officer should provide guidance to managers on the responsibilities and specific procedures that should be followed. ISF SoGP SG1.1 requires that a full time chief information security officer be appointed in the organisation, while ISF SoGP SR2.1 requires the establishment of a high-level working group to manage information privacy issues.

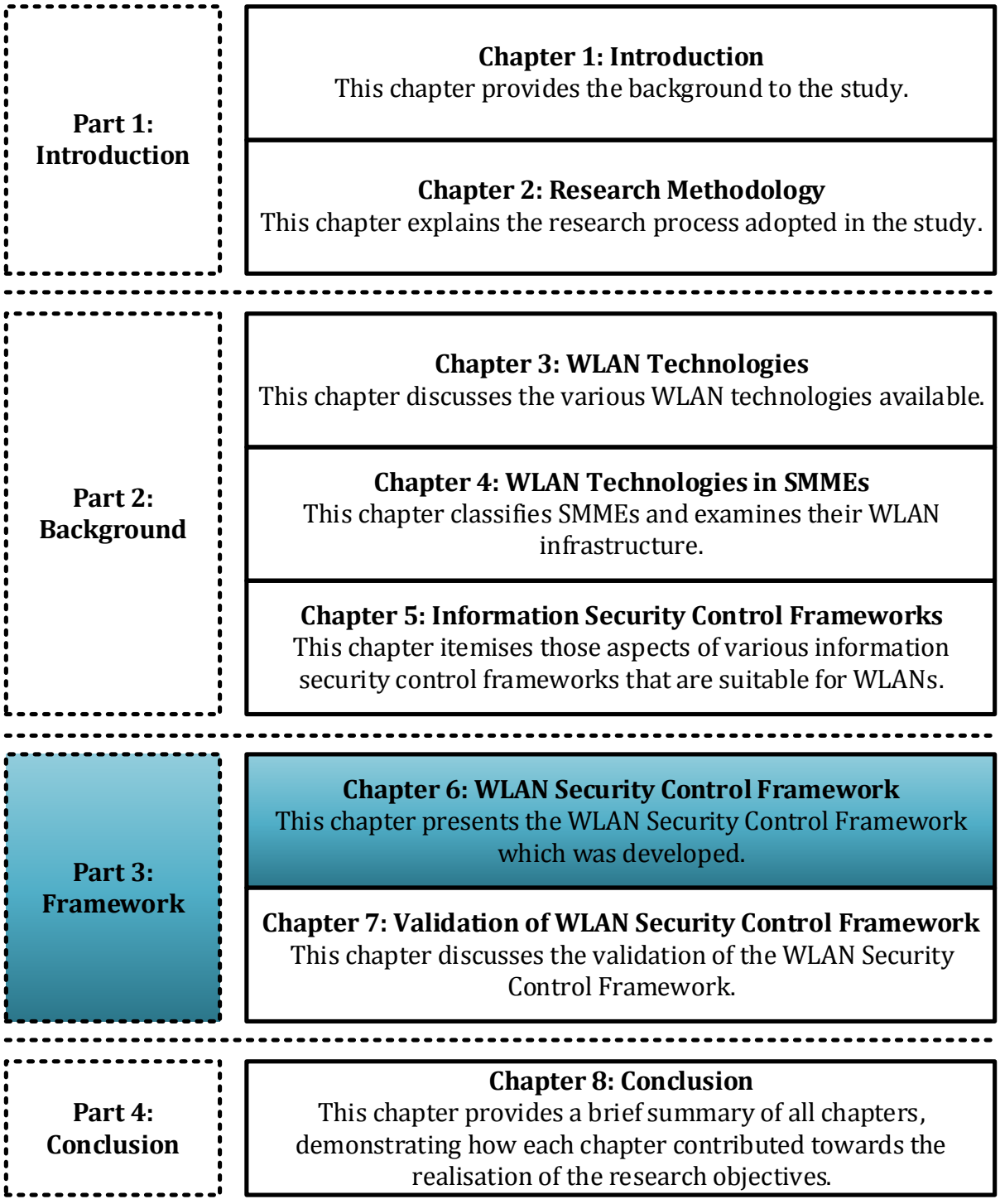
While such specialised information security personnel may be found in larger organisations, small organisations would not, typically, have an employee dedicated to these tasks.

## 5.4 Conclusion

The information security control frameworks researched in this study were not created specifically for small, medium, and micro enterprises (SMMEs). The frameworks are exhaustive and, therefore, they are not suitable for SMMEs. In addition, they are aimed at larger corporations and are also not freely available, thus extensive resources are required in order to purchase them. The controls in the frameworks are typically aimed at experienced security professionals such as information security officers. They are also too complex for the ordinary SMME staff to understand and implement. Finally, the control frameworks are not specifically related to securing WLANs although there may be a few controls that may be applicable.

This chapter has presented and examined various control frameworks that are used for information security. The next chapter highlights certain aspects of these frameworks in view of their relevance to the securing of WLAN implementations and they are used in the development of the WLAN Security Control Framework which is also presented in the next chapter.

# 6 WLAN Security Control Framework



## 6.1 Introduction

This chapter presents the proposed Wireless Local Area Network (WLAN) Security Control Framework. The WLAN Security Control Framework is a framework that small, medium and micro sized enterprises (SMMEs) may use to improve their WLAN security status.

The framework helps SMMEs to secure their WLANs against the escalating threats of malware, hacking, social engineering, misuse, physical threats, error threats and environmental threats.

Section 6.2 contains an explanation of the way in which the WLAN Security Control Framework was developed. Section 6.3 assesses the various information security control framework standards that were identified in Chapter 5 as being relevant to the WLAN Security Control Framework. The result of this assessment is a set of applicable components which is presented in section 6.4. Section 6.5 discusses the structure of the WLAN Security Control Framework while section 6.6 presents the framework itself. Section 6.7 contains an explanation of how to use the framework using the Plan-Do-Check-Act cycle, while section 6.8 concludes the chapter.

## 6.2 The Development of the Framework

In order to construct the WLAN Security Control Framework, the following process was followed (see Figure 6.1):

- Some of the existing information security control framework standards were described in Chapter 5.
- The security requirements for WLANs were discussed in Chapter 3.
- The information technology and network requirements for SMMEs were discussed in Chapter 4.
- Using the above information, an assessment was conducted on the information security control frameworks selected to identify which components would be applicable when securing WLANs in SMMEs. This exercise is depicted in Tables 6.1, 6.2, and 6.3 for Control Objectives for Information and Related Technology 5 for Information Security (COBIT 5), International Organisation for Standardisation and the International Electro-technical Commission 27002:2005

(ISO 27002), and Information Security Forum Standard of Good Practice 2012 (ISF SoGP) respectively.

- The applicable components of the information security control frameworks were then extracted and are depicted in Tables 6.4, 6.5, and 6.6 for COBIT 5, ISO 27002, and ISF SoGP respectively.
- New controls were designed for the securing of WLANs in SMMEs using the WLAN threats and SMME classifications as identified in Chapters 3 and 4 respectively. These new controls are presented in a control matrix in Table 6.7 and are classified under Physical Security, Technical Security, and Operational Security.
- A WLAN Security Control Framework is depicted in Table 6.8 (Physical Security), Table 6.9 (Technical Security) and Table 6.10 (Operational Security).
- Finally, the WLAN Security Control Framework is validated in Chapter 7.

The next sections of this chapter will discuss this process in more detail.

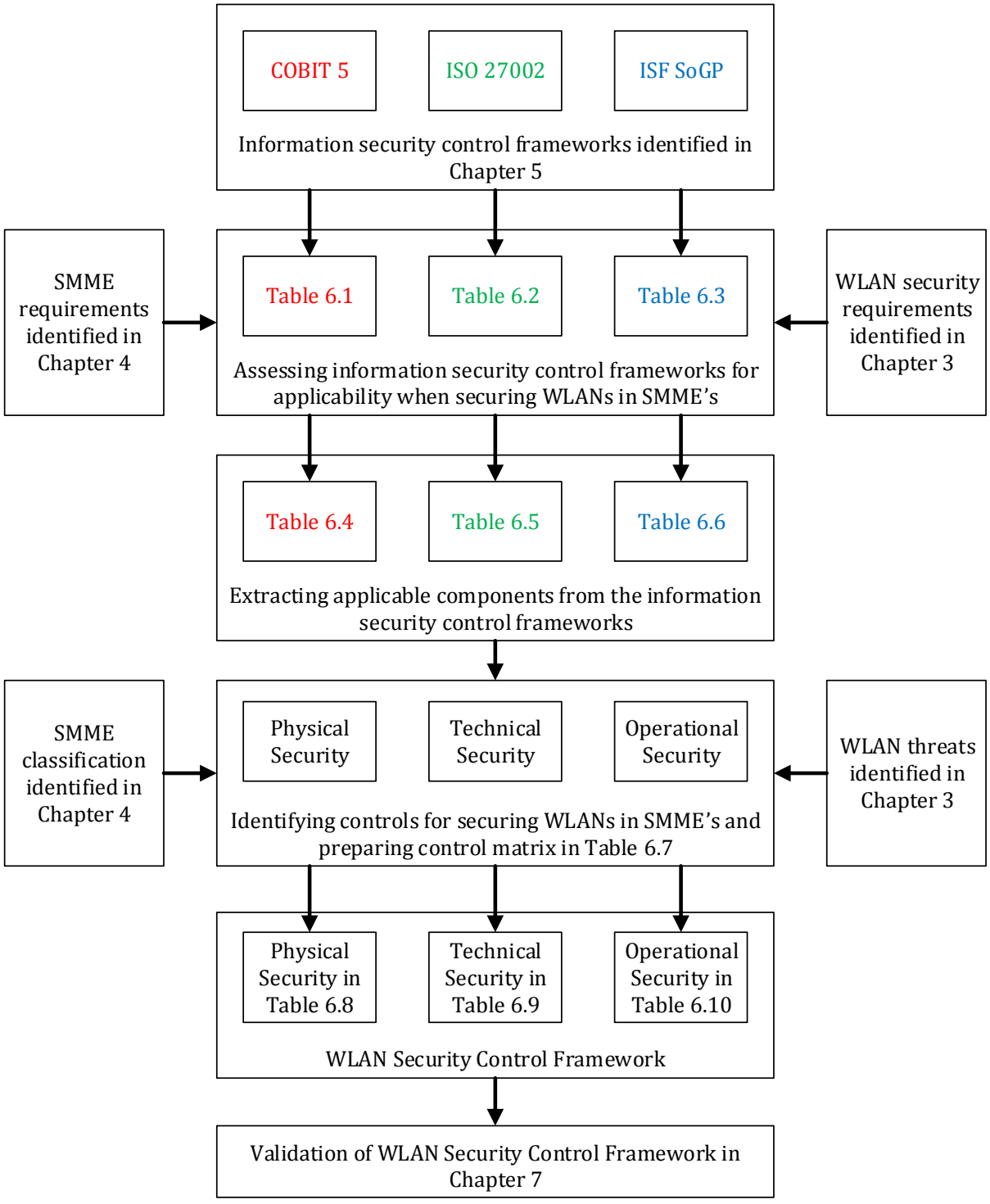



Figure 6.1: Process for developing the WLAN Security Control Framework

## 6.3 Assessing Control Frameworks for Applicability

Three information security control frameworks, as identified in Chapter 5, were assessed to identify which controls were applicable to the securing of WLANs in SMMEs.

The first framework that was assessed was COBIT 5 and is presented in Table 6.1. The domains from COBIT 5 that were deemed applicable to the securing of WLANs in SMMEs are denoted as such in the table.

Based on the discussion contained in Chapter 4 a number of items were deemed not applicable. For example, EDM02 in Table 6.1 was not deemed applicable to the securing of WLANs for SMMEs in view of the prior suggestion that, in general, SMMEs do not have at their disposal the resources for large investments in security.

Table 6.1: COBIT 5 domains assessed for applicability when securing WLANs in SMMEs

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| EDM01: Ensure Governance Framework Setting and Maintenance | **Y** | EDM01 ensures that the information security governance system is embedded in the enterprise and assurance is obtained as regards the information security governance system. EDM01 is applicable to WLAN security in SMMEs because it requires that an SMME addresses WLAN security as a critical business issue. |
| EDM02: Ensure Benefits Delivery | **N** | EDM02 ensures that the benefits, costs, and risks of information security investments are both balanced and managed and contribute optimal value. EDM02 is not applicable to WLAN security in SMMEs. |
| EDM03: Ensure Risk Optimisation | **N** | EDM03 ensures that information risk management is part of the overall enterprise risk management. EDM03 is not applicable to WLAN security in SMMEs. |
| EDM04: Ensure Resource Optimisation | **N** | EDM04 ensures that information security resources are optimised and that information security resources are in alignment with business requirements. EDM04 is not applicable to WLAN security in SMMEs. |
| EDM05: Ensure Stakeholder Transparency | **N** | EDM05 ensures that stakeholders are informed of the current status of information security and information risk throughout the enterprise. EDM05 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| APO01: Manage the IT Management Framework | **Y** | APO01 ensures the alignment of information security with the information technology (IT) and business frameworks operating in the enterprise. APO01 is applicable to WLAN security in SMMEs because it requires that a WLAN security policy be documented and signed off by management. |
| APO02: Manage Strategy | **N** | APO02 ensures that a comprehensive information security strategy is in place and is aligned with the overall enterprise and IT strategy. APO02 is not applicable to WLAN security in SMMEs. |
| APO03: Manage Enterprise Architecture | **N** | APO03 ensures that the information security architecture is understood as part of the overall enterprise architecture and is aligned and evolves with changes to the enterprise architecture. APO03 is not applicable to WLAN security in SMMEs. |
| APO04: Manage Innovation | **N** | APO04 ensures that innovation in the information security programme is promoted and that information security requirements are taken into account when innovation is enabled. APO04 is not applicable to WLAN security in SMMEs. |
| APO05: Manage Portfolio | **N** | APO05 ensures that information security investments are allocated in accordance with the risk appetite and that information security programme changes are reflected in relevant IT service, asset and resource portfolios. APO05 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| APO06: Manage Budget and Costs | **N** | APO06 ensures that the allocation of the budget and costs for information security is prioritised effectively. APO06 is not applicable to WLAN security in SMMEs. |
| APO07: Manage Human Resources | **Y** | APO07 ensures that human resource capabilities and processes are aligned with information security requirements. APO07 is applicable to WLAN security in SMMEs because it requires that staff members be trained on the general risks of WLANs and that accounts are disabled when a staff member leaves the organisation. |
| APO08: Manage Relationships | **N** | APO08 ensures that coordination, communication and a liaison structure are established between the information security function and various other stakeholders. APO08 is not applicable to WLAN security in SMMEs. |
| APO09: Manage Service Agreements | **N** | APO09 ensures service level agreements (SLAs) take into account information security requirements. APO09 is not applicable to WLAN security in SMMEs. |
| APO10: Manage Suppliers | **N** | APO10 ensures that suppliers and contracts are assessed regularly and that appropriate risk mitigation plans are formulated. APO10 is not applicable to WLAN security in SMMEs. |
| APO11: Manage Quality | **N** | APO11 ensures that operational information security quality requirements for information security services are defined and implemented. APO11 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| APO12: Manage Risk | **N** | APO12 ensures that the information security incident response is integrated with the overall risk management process to provide the capability to update the risk management portfolio. APO12 is not applicable to WLAN security in SMMEs. |
| APO13: Manage Security | **Y** | APO13 ensures that a security plan has been put in place, accepted and communicated throughout the enterprise, as well as ensuring that information security solutions are implemented and operated consistently. APO13 is applicable to WLAN security in SMMEs because it requires that an SMME's approach to WLAN security is governed by high security standards. |
| BAI01: Manage Programmes and Projects | **N** | BAI01 ensures that information security requirements are considered and incorporated in all programmes and projects. BAI01 is not applicable to WLAN security in SMMEs. |
| BAI02: Manage Requirements Definition | **N** | BAI02 ensures that all relevant information security aspects of business, functional and technical requirements are identified and implemented. BAI02 is not applicable to WLAN security in SMMEs. |
| BAI03: Manage Solutions Identification and Build | **N** | BAI03 ensures that information security measures are embedded in the solution and effectively support the business strategic and operational objectives. BAI03 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| BAI04: Manage Availability and Capacity | **Y** | BAI04 ensures that information security requirements are included in the availability, performance and capacity management plans. BAI04 is applicable to WLAN security in SMMEs because it requires that SMMEs deploy redundant access points throughout their offices. |
| BAI05: Manage Organisational Change Enablement | **N** | BAI05 ensures that information security alerts and trends are used effectively both to enable change in the enterprise and to influence the enterprise information security culture. BAI05 is not applicable to WLAN security in SMMEs. |
| BAI06: Manage Changes | **N** | BAI06 ensures that information security requirements are incorporated during impact assessments of processes, applications and infrastructure changes. BAI06 is not applicable to WLAN security in SMMEs. |
| BAI07: Manage Change Acceptance and Transitioning | **N** | BAI07 ensures that information security testing is an integral component of acceptance testing and that the information security improvements identified are incorporated in future releases of software. BAI07 is not applicable to WLAN security in SMMEs. |
| BAI08: Manage Knowledge | **N** | BAI08 ensures that knowledge sharing within an organisation is supported with the proper safeguards. BAI08 is not applicable to WLAN security in SMMEs. |
| BAI09: Manage Assets | **N** | BAI09 ensures that all assets acquired meet information security requirements. BAI09 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| BAI10: Manage Configuration | **Y** | BAI10 ensures that information security configuration baselines are approved, implemented and maintained throughout the enterprise. BAI10 is applicable to WLAN security in SMMEs because it requires that WLAN information and firmware software are stored in a secure place in order to facilitate repairs to access points and client devices. |
| DSS01: Manage Operations | **Y** | DSS01 ensures that information security operations are performed in accordance with an information security operational plan. DSS01 is applicable to WLAN security in SMMEs because it requires that SMMEs protect WLAN access points to ensure that business operations are able to continue in the event of an incident. |
| DSS02: Manage Service Requests and Incidents | **N** | DSS02 ensures that an effective information security incident response programme is established and maintained. DSS02 is not applicable to WLAN security in SMMEs. |
| DSS03: Manage Problems | **N** | DSS03 ensures that information security problems are solved in a sustainable way. DSS03 is not applicable to WLAN security in SMMEs. |
| DSS04: Manage Continuity | **Y** | DSS04 ensures that information risk is properly identified and addressed in the information and communications technology continuity plan. DSS04 is applicable to WLAN security in SMMEs because it requires that SMMEs formulate a data |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| | | backup plan for WLAN devices in case of failure and which will allow for quick recovery. |
| DSS05: Manage Security Services | **Y** | DSS05 ensures that the information processed on, stored on and transmitted by endpoint devices is protected. DSS05 is applicable to WLAN security in SMMEs because it requires that all users are uniquely identifiable and that they have access rights in accordance with their business roles. In addition, it requires that physical measures be implemented to protect information from unauthorised access, damage and interference when being processed, stored or transmitted. It also requires that electronic information is properly secured when stored, transmitted or destroyed. |
| DSS06: Manage Business Process Controls | **Y** | DSS06 ensures that appropriate controls over information security processes are in place, reviewed and updated. DSS06 is applicable to WLAN security in SMMEs because it requires that processes are in place to distribute WLAN security keys in a secure way. |
| MEA01: Monitor, Evaluate and Assess Performance and Conformance | **N** | MEA01 ensures that information security performance is monitored on an ongoing basis. MEA01 is not applicable to WLAN security in SMMEs. |

| COBIT 5 DOMAINS | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| MEA02: Monitor, Evaluate and Assess the System of Internal Control | **Y** | MEA02 ensures that information security controls are deployed and that they operate effectively. MEA02 is applicable to WLAN security in SMMEs because it requires that access points are audited on a regular basis and log files are reviewed. |
| MEA03: Monitor, Evaluate and Assess Compliance with External Requirements | **N** | MEA03 ensures that information security and information risk practices conform to external compliance requirements. MEA03 is not applicable to WLAN security in SMMEs. |

The second framework that was assessed was ISO 27002 – See Table 6.2. The control clauses from ISO 27002 that were deemed to be applicable to the securing of WLANs in SMMEs are denoted as such in the table.

As mentioned before, on the basis of the discussion in Chapter 4, some items were deemed not to be applicable.

Table 6.2: ISO 27002 Control clauses assessed for applicability when securing WLANs in SMMEs

| ISO 27002 CONTROL CLAUSES | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| A.5: Security Policy | **Y** | A.5 ensures that management direction and support for information security are provided in accordance with business requirements as well as relevant laws and |

| ISO 27002 CONTROL CLAUSES | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| | | regulations. A.5 is applicable to WLAN security in SMMEs because it requires that an SMME's overall approach to WLAN security supports high standards of governance and also that a WLAN security policy be documented and signed off by management. |
| A.6: Organisation Information Security | **N** | A.6 ensures that a management framework is established to initiate and control the implementation of information security within the organisation and maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. A.6 is not applicable to WLAN security in SMMEs. |
| A.7: Asset Management | **Y** | A.7 ensures that all assets are accounted for and have a nominated owner. It also ensures that information is classified to indicate the need, priorities, and expected degree of protection when such information is handled. A.7 is applicable to WLAN security in SMMEs because it requires that suitable controls are in place to protect WLAN devices from loss or theft. |
| A.8: Human Resources Security | **Y** | A.8 ensures that employees, contractors and third party users understand their responsibilities, are equipped to support organisational security policies, and exit an organisation or change employment in an orderly manner. A.8 is applicable to WLAN security in SMMEs because it requires that staff be trained in the general |

| ISO 27002 CONTROL CLAUSES | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| | | risks of WLANs and that accounts are disabled when a staff member leaves the organisation. |
| A.9: Physical and Environmental Security | **Y** | A.9 ensures the prevention of unauthorised physical access, damage, and interference to the organisation's premises and information. A.9 is applicable to WLAN security in SMMEs because it requires that WLAN equipment is secured against malicious users gaining physical access. |
| A.10: Communications and Operations Management | **Y** | A.10 ensures the correct and secure operation of information processing facilities, the appropriate level of information security and service delivery in line with third party service delivery agreements, the minimised risk of system failures, the integrity of software and information, the protection of information in networks, and the security of electronic commerce services. A.10 is applicable to WLAN security in SMMEs because it requires that authentication be configured, WLAN access points are kept up to date, and WLAN information is secured. |
| A.11: Access Control | **Y** | A.11 ensures that access to information is controlled and that unauthorised access is prohibited. A.11 is applicable to WLAN security in SMMEs because it requires that multiple access control (MAC) address filtering is applied, strong WLAN passwords are configured, and management interfaces on WLAN access points are secured. |

| ISO 27002 CONTROL CLAUSES | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| A.12: Information Systems Acquisition, Development and Maintenance | **Y** | A.12 ensures that security is an integral aspect of information systems and prevents errors, loss, unauthorised modification or misuse of information in applications. A.12 is applicable to WLAN security in SMMEs because it requires that WLAN device firmware is updated regularly. |
| A.13: Information Security Incident Management | **N** | A.13 ensures that information security events and weaknesses associated with information systems are communicated in a manner which allows timely corrective action to be taken. A.13 is not applicable to WLAN security in SMMEs. |
| A.14: Business Continuity Management | **Y** | A.14 ensures that interruptions to business activities are counteracted and protects critical business processes from the effects of either major failures of information systems or disasters. A.14 is applicable to WLAN security in SMMEs because it requires redundant WLAN devices be deployed to improve availability of systems as well as data backups and that recovery plans are put in place in the event of errors occurring. |
| A.15: Compliance | **Y** | A.15 ensures that all breaches of any law, statutory, regulatory or contractual obligations are avoided and that security audits maximise effectiveness and minimise interferences. A.15 is applicable to WLAN security in SMMEs because it requires that WLAN access points be audited regularly to ensure authorised personnel only are using the WLAN. |

The third and final framework that was assessed was ISF SoGP, which is presented in Table 6.3. The security areas from ISF SoGP that were deemed applicable to the securing of WLANs in SMMEs are denoted as such in the table.

As mentioned before, based on the discussion in Chapter 4, some items were deemed not to be applicable.

Table 6.3: ISF SoGP assessed for applicability when securing WLANs in SMME's.

| **ISF SoGP SECURITY AREA** | **DEEMED APPLICABLE (Y/N)** | **DISCUSSION** |
|---|---|---|
| SG1: Security Governance Approach | **Y** | SG1 ensures that an organisation's overall approach to information security supports high standards of governance and provides a top-down management structure for co-ordinating security. SG1 is applicable to WLAN security in SMMEs because it requires that an SMME's overall approach to WLAN security supports high standards of governance. |
| SG2: Security Governance Components | **N** | SG2 ensures that the information security programme contributes to the organisation's success and delivers value to the stakeholders as well as providing assurance that information risk is being adequately addressed. SG2 is not applicable to WLAN security in SMMEs. |
| SR1: Information Risk Assessment | **N** | SR1 enables individuals who are responsible for target environments to identify key information risks and determine the controls required to keep those risks within acceptable limits. SR1 is not applicable to WLAN security in SMMEs. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| SR2: Compliance | **N** | SR2 addresses compliance with the laws and regulations on information security and the prevention of information about individuals being used in an inappropriate manner. SR2 is not applicable to WLAN security in SMMEs. |
| CF1: Security Policy and Organisation | **Y** | CF1 ensures that the documenting of the governing body's direction on and commitment to information security and ensuring good practice in information security is applied effectively and consistently throughout the organisation. CF1 is applicable to WLAN security in SMMEs because it requires that a WLAN security policy be documented and signed off by management. |
| CF2: Human Resource Security | **Y** | CF2 ensures that staff members behave in a manner which is in accordance with the organisation's information security policy and information security strategy by creating a security-positive culture in which all relevant individuals apply security controls and prevent critical and sensitive information from being compromised. CF2 is applicable to WLAN security in SMMEs because it requires that staff members be trained on the general risks of WLANs and that accounts are disabled when a staff member leaves the organisation. |
| CF3: Asset Management | **N** | CF3 determines the level of protection that should be applied to particular types of information and the prevention of unauthorised disclosure as well as |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| | | supporting risk-based decisions regarding hardware and software. CF3 is not applicable to WLAN security in SMMEs. |
| CF4: Business Applications | **N** | CF4 ensures business applications use consistent security functionality that aligns with the organisation's technical security infrastructure. CF4 is not applicable to WLAN security in SMMEs. |
| CF5: Customer Access | **N** | CF5 ensures that all aspects of customer access to the organisation's business applications meet security requirements as well as ensuring that customers are legally and contractually bound to protect the organisation's information. CF5 is not applicable to WLAN security in SMMEs. |
| CF6: Access Management | **Y** | CF6 ensures that authorised individuals only are able to gain access to business applications, information systems, networks and computing devices, that individual accountability is assured and that authorised users are granted access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority. CF6 is applicable to WLAN security in SMMEs because it requires that authentication and strong passwords are configured on the WLAN. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| CF7: System Management | **Y** | CF7 ensures that computer system, network and telecommunication installations meet the security requirements of the critical business applications they support and that changes are applied correctly and do not compromise the security of business applications, computer systems or networks. CF7 is applicable to WLAN security in SMMEs because it requires that backups of configurations are securely stored and that WLAN security keys are distributed when they are changed. |
| CF8: Technical Security Infrastructure | **Y** | CF8 enables system developers and administrators to implement consistent, simple-to-use security functionality across multiple business applications and computer systems throughout the organisation. CF8 is applicable to WLAN security in SMMEs because it requires that user identification is performed. This, in turn, allows for the improved auditing of user activity. |
| CF9: Network Management | **Y** | CF9 ensures that the configuration of network devices is accurate and does not compromise the security of the network and that networks are configured accurately and securely. CF9 is applicable to WLAN security in SMMEs because it requires that WLAN access points are secured, WLAN site surveys are conducted on a regular basis and MAC address filtering is configured. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| CF10: Threat and Vulnerability Management | **Y** | CF10 addresses technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and, consequently, having a serious impact on business. CF10 is applicable to WLAN security in SMMEs because it requires that the firmware of WLAN devices is updated regularly and log files are regularly reviewed. |
| CF11: Incident Management | **N** | CF11 ensures that information security incidents are identified and resolved quickly and effectively, thus minimising their business impact and reducing the risk of similar incidents occurring. CF11 is not applicable to WLAN security in SMMEs. |
| CF12: Local Environments | **N** | CF12 provides a high-level picture of the type and importance of the business conducted in the local environment. This, in turn, helps to support security decisions about activities relating to the local environment. CF12 is not applicable to WLAN security in SMMEs. |
| CF13: Desktop Applications | **N** | CF13 ensures that accurate and up-to-date records of critical desktop applications are maintained, thus enabling them to be protected accordingly. CF13 is not applicable to WLAN security in SMMEs. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| CF14: Mobile Computing | **Y** | CF14 ensures that critical and sensitive information handled by staff members working in remote environments is protected against the full range of security threats. CF14 is applicable to WLAN security in SMMEs because it requires that WLAN client devices are encrypted and secured so as to provide protection against unauthorised individuals. |
| CF15: Electronic Communications | **N** | CF15 ensures that messaging services are available when required, the confidentiality and integrity of messages are protected in transit, and the risk of misuse is minimised. CF15 is not applicable to WLAN security in SMMEs. |
| CF16: External Supplier Management | **N** | CF16 ensures that critical and sensitive information is protected when being handled by external suppliers or when being transmitted between the organisation and the supplier. CF16 is not applicable to WLAN security in SMMEs. |
| CF17: System Development Management | **N** | CF17 ensures that business applications (including those under development) meet business and information security requirements. CF17 is not applicable to WLAN security in SMMEs. |
| CF18: System Development Lifecycle | **N** | CF18 ensures that systems are produced based on sound design principles and with security functionality built in, thus enabling controls to be incorporated easily, and withstand malicious attacks. CF18 is not applicable to WLAN security in SMMEs. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| CF19: Physical and Environment Security | **Y** | CF19 ensures physical access is restricted to authorised individuals, ensures that critical equipment is available when required and helps to prevent important services from being disrupted by the loss of, or damage to, equipment or facilities. CF19 is applicable to WLAN security in SMMEs because it requires that WLAN equipment is secured against malicious users gaining physical access. |
| CF20: Business Continuity | **Y** | CF20 enables the organisation to withstand the prolonged unavailability of critical information, business applications and related technical infrastructure, and provides individuals with a documented set of actions to perform in the event of a disaster. CF20 is applicable to WLAN security in SMMEs because it requires that redundant WLAN devices be deployed to improve availability as well as data backups and that recovery plans be put in place in case errors occur. |
| SI1: Security Audit | **Y** | SI1 ensures that security controls have been implemented effectively and that risk is being managed. In addition, it provides the owners of target environments and executive management with an independent assessment of their security status. SI1 is applicable to WLAN security in SMMEs because it requires that WLAN access points are regularly audited by authorised personnel. |

| ISF SoGP SECURITY AREA | DEEMED APPLICABLE (Y/N) | DISCUSSION |
|---|---|---|
| SI2: Security Performance | **N** | SI2 provides executive management with an accurate, comprehensive and coherent assessment of the information security status of the organisation. SI2 is not applicable to WLAN security in SMMEs. |

## 6.4 COBIT 5, ISO 27002 and ISF SoGP Applicable Components

This section summarises the extracted components from COBIT 5, ISO 27002, and ISF SoGP that were deemed to be applicable when securing WLANs in SMMEs. The processes and procedures of the extracted components were used in the development of the WLAN Security Control Framework.

The COBIT 5 processes that were deemed to be applicable to the WLAN Security Control Framework are listed in Table 6.4:

Table 6.4: COBIT 5 Domains and processes applicable to the WLAN Security Control Framework

| COBIT 5 DOMAIN | APPLICABLE COBIT 5 PROCESSES |
|---|---|
| **Evaluate, Direct and Monitor** | EDM01: Ensure Governance Framework Setting and Maintenance |
| **Align, Plan and Organise** | APO01: Manage the IT Management Framework<br>APO07: Manage Human Resources<br>APO13: Manage Security |
| **Build, Acquire and Implement** | BAI04: Manage Availability and Capacity<br>BAI10: Manage Configurations |
| **Deliver, Service and Support** | DSS01: Manage Operations<br>DSS04: Manage Continuity<br>DSS05: Manage Security Services<br>DSS06: Manage Business Process Controls |
| **Monitor, Evaluate and Assess** | MEA02: Monitor, Evaluate and Assess the System of Internal Control |

The ISO 27002 main security categories that were deemed to be applicable to the WLAN Security Control Framework are listed in Table 6.5:

Table 6.5: ISO 27002 Security clauses applicable to the WLAN Security Control Framework

| ISO 27002 CLAUSE |
|---|
| **A.5:** Security Policy |
| **A.7:** Asset Management |

| |
|---|
| **A.8:** Human Resource Security |
| **A.9:** Physical and Environmental Security |
| **A.10:** Communications and Operations Management |
| **A.11:** Access Control |
| **A.12:** Information Systems Acquisition, Development and Maintenance |
| **A.14:** Business Continuity Management |
| **A.15:** Compliance |

The ISF SoGP topics that were deemed to be applicable to the WLAN Security Control Framework are listed in Table 6.6:

Table 6.6: ISF SoGP Categories and areas applicable to the WLAN Security Control Framework

| ISF SoGP CATEGORIES | APPLICABLE ISF SoGP AREAS |
|---|---|
| **SG: Security Governance** | SG1: Security Governance |
| **CF: Control Framework** | CF1: Security Policy and Organisation<br>CF2: Human Resource Security<br>CF6: Access Management<br>CF7: System Management<br>CF8: Technical Security Infrastructure<br>CF9: Network Management<br>CF10: Threat and Vulnerability Management<br>CF14: Mobile Computing<br>CF19: Physical and Environmental Security<br>CF20: Business Continuity |
| **SI: Security Monitoring and Improvement** | SI1: Security Audit |

Each of the components identified in the information security control frameworks (COBIT 5, ISO 27002 and ISF SoGP) influenced the development of the WLAN Security Control Framework. The next section discusses the structure of the framework.

## 6.5 WLAN Security Control Framework Structure

In order to explain the way in which the WLAN Security Control Framework was developed, a walkthrough is conducted below.

1. Take the example of "APO07: Manage Human Resources" from COBIT 5 as presented in Table 6.4.
2. APO07 was taken into account when a control activity for securing WLANs in SMMEs was created. This control activity was defined as "Train staff on the general risks of WLANs".
3. The following control objective was then derived, namely, "To provide staff members with the skills required to protect against the general risks of WLANs" and a detailed description was provided for the control activity.
4. A decision was made regarding the general security area under which this control objective could be categorised, namely, physical security, technical security, or operational security.
5. A reference code was added to the control activity name – in this case "PS04" as it was deemed to fall under physical security (PS).
6. A relevance indication was added, for example Fundamental (F) if it were applicable to all organisations or Specialised (S) if it were applicable to specific organisations only. PS04 was deemed to be of fundamental relevance.
7. A SMME classification was provided to indicate whether it is applicable to micro, small and/or medium enterprises. PS04 was deemed to be applicable to small and medium enterprises.
8. The threats that may possibly be mitigated by this control activity were indicated. For example, PS04 may mitigate social engineering, physical, and environmental threats.
9. Finally, all the original information security control framework references were provided to enable the reader to investigate further details of the control activity. In this case, APO07 from COBIT 5 was similar to A.8 and A.9 from ISO 27002, and CF2 from ISF SoGP.
10. These steps were repeated for all the COBIT 5 domains, ISO 27002 clauses, and ISF SoGP categories which had been deemed to be applicable to the securing of WLANs in SMMEs.

All of the information described above is included in Table 6.7, which presents a summary control matrix for the WLAN Security Control Framework. Further detailed information for the thirty-six control activities created is included in Tables 6.8, 6.9, and 6.10 which list the Physical Security (PS), Technical Security (TS), and Operational Security (OS) detail for the framework respectively.

*Note: The order of the security areas in this WLAN Security Control Framework does not imply their importance. All security areas are important and, thus, it is recommended that organisations apply the control activities that are applicable to their size.*

Figure 6.2 depicts the links between the information security control frameworks and the three security areas. All the control frameworks possessed components that were relevant to all the security areas used in the WLAN Security Control Framework.

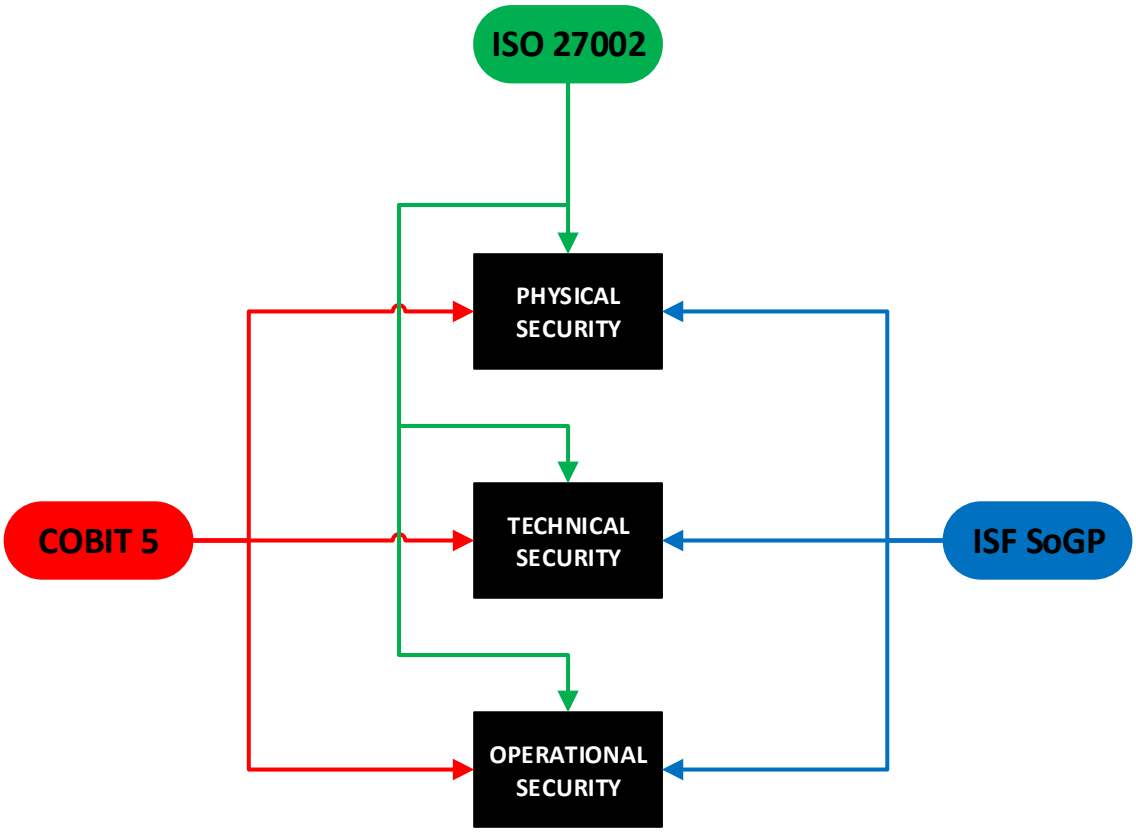



Figure 6.2: From information security control frameworks to security areas as adopted in the WLAN Security Control Framework

The following subsections explain the components of the WLAN Security Control Framework in more detail.

### 6.5.1 Reference

Each control activity in the WLAN Security Control Framework has a unique reference. These references include the security area under which the control activity falls and also the 2 digit number of the control activity (e.g. PS05 means Physical Security control number 05).

### 6.5.2 Control Activity Name

Each control activity is given a unique name that summarises the control description (i.e. PS05 – Control access to secure areas).

### 6.5.3 Security Relevance

The WLAN Security Control Framework makes a distinction between those control activities that are considered Fundamental (F) and those that are considered Specialised (S). The aim of this classification is to make it easier to identify the essential security arrangements that are likely to be relevant for most organisations and to distinguish such essential security arrangements from those that depend on other factors that are not universal.

- FUNDAMENTAL controls are the WLAN security arrangements that are generally applied by organisations to form the foundation of their wireless security.
- SPECIALISED controls are those WLAN security arrangements that depend on how or in what environment the SMME operates and are not typically relevant to most organisations.

*PS04 is an example of a FUNDAMENTAL control is and PS05 is an example of a SPECIALISED control.*

### 6.5.4 Organisation Classification

The control activities are classified as Micro, Small or Medium. This classification is used to distinguish the different levels of WLAN security requirements for SMMEs. The classifications are marked in the control matrix with a tick (✓) to enable to SMMEs to identify which controls are relevant to their organisations easily. The classification specifications of SMMEs were discussed in detail in Chapter 4.

### 6.5.5 Threats Mitigated

The threats mitigated component of the WLAN Security Control Framework advises the SMME on the risks which are reduced when the security control is applied. The following threats are described in detail in Chapter 3.

- **Malware threats** – The threat of malware to a WLAN is caused by malicious software which has been developed for the purpose of compromising information and harming WLAN devices.
- **Hacking threats** – The threats of WLANs being hacked involve unauthorised external individuals deliberately attempting to access or harm an organisation's network by exploiting vulnerabilities and bypassing security controls.
- **Social engineering threats** – The threat of social engineering involves the use of social tactics to exploit an individual and influence him/her to perform specific actions such as disclosing WLAN authentication information.
- **Misuse threats** – The threat of misuse involves the unauthorised use of resources and privileges to gain access to information on a WLAN.
- **Physical threats** – Physical threats are typically associated with the loss or theft of WLAN equipment.
- **Error threats** – Error threats to WLANs are usually the result of one or more individuals making mistakes.
- **Environmental threats** – Environmental threats are typically associated with WLANs being affected by natural events, such as floods or storms, or man-made events, such as fires, explosions, riots or electrical interference.

The threats mitigated are marked in the control matrix with a tick (✓).

### 6.5.6 Control Objective

Control objectives indicate what the control activities are trying to achieve, for example, PS05: To restrict access to secure areas to authorised personnel only by ensuring that individuals who are not authorised to access secure areas do not have such access).

### 6.5.7 Control Description

The control description provides more detail on the control activity, including the steps that should be taken to implement the control.

### 6.5.8 Reference to Information Security Control Frameworks

Information security control frameworks were used as a source of information in order to construct the WLAN Security Control Framework. The WLAN Security Control Framework is referenced to these international standards so that, if required, more information on the topics may be found.

## 6.6 WLAN Security Control Framework

This section presents the WLAN Security Control Framework for SMMEs. As mentioned earlier in this chapter, the framework consists of a control matrix table and detailed control tables for physical, technical and operational security.

Table 6.7: Control matrix for the WLAN Security Control Framework

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| **PHYSICAL SECURITY** | | | | | | | | | | | | |
| **PS01** | **Secure antennae and related cabling supporting WLANs.** | F | | | ✓ | | ✓ | | | ✓ | | ✓ |
| **PS02** | **Secure WLAN access points.** | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| **PS03** | **Secure WLAN client devices.** | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| **PS04** | **Train staff members on the general risks of WLANs.** | F | | ✓ | ✓ | | | ✓ | | ✓ | | ✓ |
| **PS05** | **Control access to secure areas.** | S | | | ✓ | | | ✓ | | ✓ | | ✓ |
| **PS06** | **Conduct regular WLAN site surveys.** | S | | | ✓ | | ✓ | ✓ | | | | |
| **PS07** | **Secure antennae so as to minimise coverage.** | F | | | ✓ | | ✓ | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PS08** | **Deploy redundant WLAN access points.** | F | | ✓ | ✓ | | | | | ✓ | | ✓ |
| **PS09** | **Secure backups.** | F | | | ✓ | | | | ✓ | ✓ | ✓ | ✓ |
| **PS10** | **Protect WLAN access points with UPS.** | F | | | ✓ | | | | | | ✓ | ✓ |
| **TECHNICAL SECURITY** | | | | | | | | | | | | |
| **TS01** | **Secure the SSID.** | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | |
| **TS02** | **Configure authentication.** | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| **TS03** | **Configure MAC address filtering.** | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| **TS04** | **Secure default WLAN access point settings.** | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| **TS05** | **Require a valid password prior to administrator access.** | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | ✓ | |
| **TS06** | **Configure user accounts.** | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| **TS07** | **Disable unused and dormant user accounts.** | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| **TS08** | **Configure strong passwords.** | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | |
| **TS09** | **Disable responses to broadcast SSID probe.** | S | | | ✓ | | ✓ | | | | | |
| **TS10** | **Perform user identification.** | F | | ✓ | ✓ | | ✓ | | ✓ | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **TS11** | **Segregate WLANs from internal network.** | F | | | ✓ | ✓ | ✓ | | | | | |
| **TS12** | **Secure gateways prior to accessing the internal network.** | F | | | ✓ | ✓ | ✓ | | | | | |
| **TS13** | **Secure management interface on WLAN access points.** | F | | | ✓ | | ✓ | | ✓ | | | |
| **TS14** | **Secure SNMP.** | F | | | ✓ | | ✓ | | ✓ | | | |
| **TS15** | **Enable WPA2 encryption.** | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| **TS16** | **Encrypt WLAN devices.** | F | | | ✓ | | ✓ | | | ✓ | | |
| **TS17** | **Encrypt data using high level protocols.** | F | | | ✓ | | ✓ | | | | | |
| **TS18** | **Update WLAN device firmware.** | F | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | |
| **OPERATIONAL SECURITY** | | | | | | | | | | | | |
| **OS01** | **Direct and monitor the WLAN Security Control Framework.** | F | | ✓ | ✓ | | | | ✓ | | | |
| **OS02** | **Document a WLAN security policy.** | F | ✓ | ✓ | ✓ | | | | ✓ | | | |
| **OS03** | **Distribute WPA2 encryption keys when changed.** | F | ✓ | ✓ | ✓ | | | | | | ✓ | |
| **OS04** | **Audit WLAN access points.** | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| **OS05** | **Review log files.** | F | | ✓ | ✓ | | ✓ | | ✓ | | ✓ | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **OS06** | **Store WLAN access point firmware versions.** | F | | | ✓ | | | | | | | ✓ | |
| **OS07** | **Store WLAN information.** | F | | | ✓ | | | | | | | ✓ | |
| **OS08** | **Establish a data backup and recovery plan.** | F | | | ✓ | | | | | ✓ | | ✓ | ✓ |

Table 6.8 presents the detailed control activities for the physical security area of the WLAN Security Control Framework.

Table 6.8: Physical security area of the WLAN Security Control Framework

| **PHYSICAL SECURITY** |
|---|
| **PS01 Secure antennae and related cabling supporting WLANs.** |
| **Control Objective**<br>To protect antennae and related cabling that support WLANs from interception or damage. |
| **Control Description**<br>Antennae and related cabling that support the WLANs should be kept in a secure area to which access is restricted to authorised personnel only. Suitable physical access controls should be in place where WLAN access points are located. The following WLAN security activities should be implemented:<br>1. Attach identification labels to antennae and cables.<br>2. Conceal the installation of antennae and cables.<br>3. Avoid routing cables through publicly accessible areas. |

4. Document diagrams to show where antennae and cables are located.

**COBIT 5: DSS05**

**ISO 27002: A.9**

**ISF SoGP: CF9, CF19**

**PS02 Secure WLAN access points.**

**Control Objective**

To prevent unauthorised users or malicious users from gaining access physically to WLAN access points.

**Control Description**

WLAN access points should be kept in a secured closet or enclosure to which access is restricted to authorised personnel only. Malicious users who gain physical access to a WLAN access point are able to bypass all network security measures. Organisations should make sure that these WLAN access points are not located in common areas such as kitchens, canteens, or open offices. The following WLAN security activities should be implemented:

1. Position the WLAN access points in secure environments (e.g. Locked rooms or cabinets).
2. Document diagrams to show where WLAN access points are located.

**COBIT 5: DSS05**

**ISO 27002: A.9**

**ISF SoGP: CF9, CF19**

**PS03 Secure WLAN client devices.**

**Control Objective**

To prevent unauthorised users or malicious users from gaining access physically to WLAN devices.

**Control Description**

WLAN client devices should be protected from loss or theft. Suitable physical controls should be in place to lock down WLAN client devices. Loss or theft of a WLAN client device should be reported immediately to a network security team or other appropriate designated group that may take the appropriate measures within the organisation. Precautions should be taken to protect all WLAN client devices and support devices connected to the WLAN.

**COBIT 5: DSS05**

**ISO 27002: A.7, A.9, A.11**

**ISF SoGP: CF14, CF19**

**PS04 Train staff members on the general risks of WLANs.**

**Control Objective**

To provide staff members with the skills required to provide protection against the general risks of WLANs.

**Control Description**

Staff members should be trained and educated on the general risks of WLANs. Staff members, including security teams, should be on the alert for trespassers with antennae, laptops or similar equipment. Such trespassers may be loitering in lobbies, parking lots or on pavements in order to intercept WLAN transmissions. Staff members should also be instructed to keep a lookout for unauthorised, rogue WLAN access points that may be installed on the organisation's premises. It is

considered uncommon for WLAN access points on an organisation's premises to be visible. The following WLAN security measures should be implemented:

1. Educate, train and promote awareness on the part of all staff members as regards WLAN risks.
2. Instruct staff members to be on the alert for rogue WLAN devices.

**COBIT 5: APO07**

**ISO 27002: A.8, A.9**

**ISF SoGP: CF2**

**PS05 Control access to secure areas.**

**Control Objective**

To restrict the access to secure areas to authorised personnel only by ensuring that individuals who are not authorised to access secure areas are not able to gain access to such areas.

**Control Description**

Access to secured areas should be controlled and logged. Mechanisms such as electronic key cards or biometrics should be required when accessing secure areas. Access to these secure areas should be audited on a regular basis to ensure that only those employees who are authorised to access such areas are able to gain access to the areas. The following security activities should be implemented:

1. Make use of physical access control mechanisms (e.g. electronic key cards or biometrics).
2. Review physical access control logs regularly.
3. Perform regular audits on physical access lists in order to secure areas.

**.COBIT 5: DSS05, MEA02**

**ISO 27002: A.9, A.11**

**ISF SoGP: CF19**

| PS06 | Conduct regular WLAN site surveys. |
|---|---|

**Control Objective**

To discover unauthorised, rogue WLAN access points on an organisation's premises.

**Control Description**

Security teams should conduct regular WLAN site surveys to identify and locate unauthorised WLAN access points. SSID (Service Set Identifier), MAC address and encryption type are some of the characteristics to consider when looking for an unauthorised WLAN access point.

**COBIT 5: DSS05**

**ISO 27002: A.10**

**ISF SoGP: CF9**

| PS07 | Secure antennae as to minimise coverage. |
|---|---|

**Control Objective**

To ensure that the organisation's WLAN signal does not stray beyond the intended transmission area.

**Control Description**

The appropriate antennae should be selected for use with WLAN access points so as to reduce stray radio frequency (RF) transmissions. The selection of the correct antennae may reduce the signal strength to the intended transmission area.

WLAN access points with dedicated, omni-directional antennas should be located in such a way as to minimise RF coverage outside of the intended transmission area.

1. Select the correct antennae as to reduce signal strength.
2. Configure low power to limit the range of antennae.
3. Place antennae in such locations so as to reduce stray RF transmissions.

**COBIT 5: DSS05**

**ISO 27002: A.10**

**ISF SoGP: CF9**

**PS08 Deploy redundant WLAN access points.**

**Control Objective**

Increasing the redundancy of WLAN access points improves the availability of the WLAN.

**Control Description**

For mission-critical WLAN access points, multiple devices should be deployed for the purposes of redundancy. In the event of a WLAN access point failure, WLAN client devices may be configured to automatically seek out another access point using the same SSID and WPA2 encryption keys.

**COBIT 5: BAI04**

**ISO 27002: A.14**

**ISF SoGP: CF9, CF20**

**PS09 Secure backups.**

| |
|---|
| **Control Objective**<br>To protect backups from access by unauthorised individuals. |
| **Control Description**<br>Backups contain sensitive configuration information, such as passwords and encryption keys, and should be accorded the same protection as the WLAN access point itself. The secured backups should be taken off-site. |
| **COBIT 5: DSS04**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF7** |
| **PS10 Protect WLAN access points with UPS.** |
| **Control Objective**<br>To protect WLAN access points against power failures. |
| **Control Description**<br>Uninterruptible Power Supplies (UPS) should be provided for the WLAN access points that are considered to be critical to business operations. These UPSs should be capable of supplying power for at least 15 minutes. |
| **COBIT 5: DSS01**<br>**ISO 27002: A.9**<br>**ISF SoGP: CF19** |

Table 6.9 presents the detailed control activities for the technical security area of the WLAN Security Control Framework.

Table 6.9: Technical security area of the WLAN Security Control Framework

| **TECHNICAL SECURITY** |
|---|
| **TS01 Secure the SSID.** |
| **Control Objective**<br>To ensure WLANs meet the security requirements of the organisation and that authorised individuals only gain access to the wireless network. |
| **Control Description**<br>The SSID used to identify a WLAN should be changed from the vendor default. Although the task of discovering an SSID is simple, default SSIDs are often an indication that a WLAN has not been secured and may entice the curious to explore. These SSIDs should not provide potentially useful information to malicious users. It is, thus, recommended that SSIDs are not set as values such as an organisation's name, address, floor or department because this may provide for an attractive target for potential intruders. |
| **COBIT 5: DSS05**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF7, CF9** |
| **TS02 Configure authentication.** |
| **Control Objective**<br>To ensure that only authorised individuals with access privileges gain access to an organisation's WLAN. |

**Control Description**

Open system authentication should be disabled and should not be used. Open system authentication is a null authentication that grants any requesting WLAN client device access to the WLAN. The following WLAN security activities should be implemented:

1. Disable open system authentication on WLAN access points.
2. Configure access control mechanisms on WLAN access points such as user authentication or device authentication.

**COBIT 5: DSS05**

**ISO 27002: A.10, A.11**

**ISF SoGP: CF6, CF8, CF9**

**TS03 Configure MAC address filtering.**

**Control Objective**

To prevent unauthorised devices from gaining access to an organisation's network.

**Control Description**

MAC address filtering should be used. MAC address filtering allows for a list of valid WLAN client devices MAC addresses to be specified. This list may be stored on either the access point itself or on a server that is consulted by the access point. WLAN client devices that are not included in this list are not allowed to associate with the WLAN.

**COBIT 5: DSS05**

**ISO 27002: A.10, A.11**

**ISF SoGP: CF9**

| TS04 | Secure default WLAN access point settings. |
|---|---|
| **Control Objective**<br>To prevent unauthorised users from gaining access to an organisation's network through default configurations. | |
| **Control Description**<br>Disable or delete all unused, vendor-supplied, default accounts for the WLAN access point's management interface. If a default account cannot be disabled or deleted, those accounts should be assigned a strong password. The following WLAN security activities should be implemented:<br>1. Disable unnecessary or insecure user accounts.<br>2. Different passwords to the default passwords set by suppliers must be set. | |
| **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6, CF7** | |
| **TS05** | **Require a valid password prior to administrator access.** |
| **Control Objective**<br>To ensure that authorised users only gain access to administrator accounts. | |
| **Control Description**<br>All WLAN access points should require and authenticate a valid password prior to privileged administrator access to the access point being granted. The following security activities should be implemented: | |

1. Configure administrative passwords in such a way that they are not displayed on screen.
2. Configure administrative password settings in such a way that they require strong characteristics.

**COBIT 5: DSS05**

**ISO 27002: A.11**

**ISF SoGP: CF6, CF14**

**TS06 Configure user accounts.**

**Control Objective**

To restrict access to an organisation's network to authorised users.

**Control Description**

Each user account, whether it represents either a person or a client device, should have a unique identifier that identifies one entity only within the organisation. The uniqueness of these accounts should be strictly maintained. Every user should have to make use of these unique identifiers prior to gaining access to the WLAN. For the purpose of effortless identification, all user accounts should include meaningful descriptions and naming conventions. This, in turn, simplifies the interpretation of the auditing reports.

Users should not share a single user ID for WLAN access. Each user should access the WLAN by using his/her unique user ID to ensure the accurate accounting of user access and actions. Each user account should be assigned a password and these passwords should comply fully with the organisation's password policies. All WLAN access points should require and authenticate a valid client device or user ID prior to access being granted to the WLAN. The following security activities should be implemented:

1. Create user accounts for each user in the organisation.

2. Configure user accounts in such a way that they include meaningful descriptions.
3. Assign passwords to user accounts.
4. Prohibit user ID sharing.
5. Review the list of user accounts on a regular basis.

**COBIT 5: DSS05, DSS06**

**ISO 27002: A.11**

**ISF SoGP: CF6**

**TS07 Disable unused and dormant user accounts.**

**Control Objective**

To ensure that user accounts are managed appropriately when employment is terminated or WLAN devices are either lost or stolen.

**Control Description**

Accounts should be deactivated within 24 hours of the notification of a status change (e.g. employee termination). User account passwords should be changed if a WLAN client device is either lost or stolen. If possible, the stolen WLAN client devices should be remotely wiped of all data. All unused and dormant user accounts should be disabled and then deleted.

**COBIT 5: APO07, DSS05**

**ISO 27002: A.8, A.11**

**ISF SoGP: CF2, CF6**

**TS08 Configure strong passwords.**

**Control Objective**

To prevent unauthorised users from gaining access to an organisation's password protected network.

**Control Description**

Password changes should be enforced periodically and, at least, every 90 days. Changing passwords on a regular basis ensures that, even if a malicious user does obtain access to a WLAN using a compromised password, then the password would be valid for a finite time only. In addition, passwords should not be reused. Disallowing password reuse prevents users from repeating their passwords when periodic changes are enforced. In order to avoid one system being compromised as a result of other systems being compromised, users should not use the same password for the WLAN that they use elsewhere (e.g. Windows).

**COBIT 5: DSS05**

**ISO 27002: A.11**

**ISF SoGP: CF6, CF8**

**TS09 Disable responses to broadcast SSID probe.**

**Control Objective**

To ensure authorised devices only gain access to an organisation's network.

**Control Description**

The responses to broadcast SSID probe requests should be disabled on the WLAN access points. The disabling of the broadcast SSID probe requests will prevent the access point from being seen by numerous site survey tools.

**COBIT 5: Not covered in COBIT 5**

**ISO 27002: Not covered in ISO 27002**

**ISF SoGP: CF9**

| **TS10** | **Perform user identification.** |
|---|---|

**Control Objective**

To restrict access to WLANs to authorised users only using user identification.

**Control Description**

User identification should be performed instead of client device identification. This provides for improved auditing especially in situations in which multiple users share a client device. A unique individual client or user identifier should be used when authenticating each client device or user. Multiple client devices or people should not share a single, common identifier.

**COBIT 5: DSS06**

**ISO 27002: A.11**

**ISF SoGP: CF6, CF8**

| **TS11** | **Segregate WLANs from internal network.** |
|---|---|

**Control Objective**

To ensure WLANs meet the security requirements of an organisation's network.

**Control Description**

WLANs should be treated as a non-trusted network, similar to the Internet. Firewalls and intrusion detection systems (IDS)

should be used to segregate the WLAN from the organisation's internal network. Network segregation should be performed by means of the physical separation of dedicated network equipment and wiring and not through using Virtual LANs (VLANs). VLANs have proven to be susceptible to attacks, potentially allowing an attacker to gain access.

**COBIT 5: DSS05**

**ISO 27002: A.11**

**ISF SoGP: CF7, CF9**

**TS12 Secure gateways prior to accessing the internal network.**

**Control Objective**

To ensure that authorised individuals only gain access to an organisation's network by authentication prior to access.

**Control Description**

Users should securely authenticate themselves to a gateway prior to gaining access to the organisation's internal network. Authentication methods include those provided by a Virtual Private Network (VPN) or a Secure Sockets Layer (SSL)-encrypted login page. Access through the gateway should be restricted to those network destinations and services only that are required. This limits possible attack routes from the external WLAN to the internal network. This implies that, if WLAN users only require access to an organisation's email server, then the WLAN does not need access to the organisation's financial systems.

**COBIT 5: DSS05**

**ISO 27002: A.10, A.11**

**ISF SoGP: CF6, CF9**

| TS13 | Secure management interface on WLAN access points. |
|---|---|

**Control Objective**

To ensure the protection of WLAN access point management interfaces.

**Control Description**

All network services listening on a WLAN access point's wireless network interface should either be disabled or have access denied from the wireless network addresses. In particular, access point management services should never be accessible via the wireless interface. Unused management server interfaces on WLAN access points should either be disabled or have restricted access. Many WLAN access points provide multiple configuration interfaces such as serial console ports, Telnet, File Transfer Protocol (FTP), etc. Access to management server interfaces should be restricted to specific hosts only and encrypted protocols should be used when communicating with these WLAN management servers in order to enhance confidentiality and provide data integrity. All access to the WLAN management server interfaces should be authenticated. The following WLAN security activities should be implemented:

1. Disable all unused management interfaces on WLAN access points.
2. Restrict management interfaces to specific hosts.
3. Authenticate all access to management interfaces.
4. Encrypt all administrative traffic to management interfaces.
5. Configure WLAN access points using the serial console interface.

**COBIT 5: DSS05**

**ISO 27002: A.10, A.11**

**ISF SoGP: CF7, CF9**

| TS14 | Secure SNMP. |
|---|---|
| **Control Objective**<br>To ensure that the configuration of the SNMP is secure and does not compromise the organisation's network. | |
| **Control Description**<br>The SNMP should be disabled if it is not required and is not being used. The latest version of the SNMP protocol should be installed and the support for earlier versions of SNMP disabled. At the time of this study the SNMP versions to be used, in order of preference, are:<br>a) SNMPv3 with authentication and privacy<br>b) SNMPv3 with authentication only<br>c) SNMPv2p with MD5 authentication<br>Predefined community strings such as "public" or "private" should be removed. SNMP community strings and passwords should be complex and reflect the principles of strong passwords. Different community strings and passwords should be used for each WLAN access point within the organisation. This requirement is particularly critical if the SNMP has read-write access to WLAN access points. WLAN access points should be configured to accept SNMP requests from specific hosts only, for example, a corporate SNMP management station. All SNMP communication should be authenticated and encrypted between the WLAN access point and management station. SNMPv3 with authentication and privacy satisfies this requirement. | |
| **COBIT 5: DSS05**<br>**ISO 27002: A.11** | |

**ISF SoGP: CF9**

| **TS15** | **Enable WPA2 encryption.** |
|---|---|

**Control Objective**

To ensure that all WLAN traffic is encrypted and protected against interception.

**Control Description**

WPA2 encryption should be enabled on all WLAN access points. Open authentication should be disabled and WLAN access points should reject unencrypted data packets. Older encryption standards, such as WEP and WPA, should not be used. WPA2 encryption keys should be changed on a regular basis. Changing WPA2 encryption keys frequently ensures confidentiality.

**COBIT 5: DSS05**

**ISO 27002: A.10, A.11**

**ISF SoGP: CF9**

| **TS16** | **Encrypt WLAN devices.** |
|---|---|

**Control Objective**

To ensure critical organisation information is encrypted and protected against unauthorised individuals.

**Control Description**

All WLAN devices that are connected to an organisation's network should be encrypted. The encryption adds an extra layer of security in the event of either the loss or theft of the WLAN device.

**COBIT 5: DSS05**

**ISO 27002: A.9**

**ISF SoGP: CF14**

| **TS17** | **Encrypt data using high level protocols.** |
|---|---|

**Control Objective**

To ensure the integrity of all WLAN data transmitted.

**Control Description**

All data transmitted across the WLAN should be encrypted using a high level encryption protocol that ensures data confidentiality. Such protocols include Secure Sockets Layer (SSL), Secure Shell (SSH) and Internet Protocol Security (IPsec) VPN tunnels.

**COBIT 5: DSS05**

**ISO 27002: A.10**

**ISF SoGP: CF9**

| **TS18** | **Update WLAN device firmware.** |
|---|---|

**Control Objective**

To ensure the latest security patches are installed on WLAN devices.

**Control Description**

WLAN access points and client device firmware should be updated regularly. This, in turn, addresses security vulnerabilities

| |
|---|
| or critical bugs that have been found while also taking advantage of new security or management features that have been added. Information Technology (IT) administrators should stay abreast of firmware patches and WLAN security announcements so that security holes and other critical bugs may be patched on a timely basis. |
| **COBIT 5: DSS05**<br>**ISO 27002: A.12**<br>**ISF SoGP: CF10** |

Table 6.10 presents the detailed control activities for the operational security area of the WLAN Security Control Framework.

Table 6.10: Operational security area of the WLAN Security Control Framework

| **OPERATIONAL SECURITY** |
|---|
| **OS01 Direct and monitor the WLAN Security Control Framework.** |
| **Control Objective**<br>To ensure that the organisation's overall approach to WLAN security supports high standards of governance. |
| **Control Description**<br>An organisation's governing body should establish, direct, monitor and communicate the WLAN Security Control Framework. By introducing the WLAN Security Control Framework the governing body would have demonstrated its commitment to WLAN security in the organisation. The following WLAN security activities should be implemented:<br>1. Treat WLAN security as a critical business issue. |

2. Appoint an individual to take overall responsibility for WLAN security.
3. Sign off the WLAN security policy.

**COBIT 5: EDM01, APO13**

**ISO 27002: A.5**

**ISF SoGP: SG1**

**OS02 Document a WLAN security policy.**

**Control Objective**

To document the governing body's direction on and commitment to WLAN security.

**Control Description**

There should be a documented WLAN security policy, signed off by the governing body, and that applies throughout the organisation. The WLAN security policy should define what WLAN security is and indicate the security principles that should be adhered to by all staff members. The following WLAN security activities should be implemented:

1. Align the WLAN security policy with other high level policies.
2. Communicate the policy to all staff members and external individuals.
3. Review the WLAN security policy on a regular basis.

**COBIT 5: APO01**

**ISO 27002: A.5**

**ISF SoGP: CF1**

**OS03 Distribute WPA2 encryption keys when changed.**

**Control Objective**

To ensure that all staff members have ongoing access to the WLAN.

**Control Description**

In order to facilitate the update of the WPA2 encryption keys used in WLANs, IT administrators should distribute the new keys to an organisation's WLAN user population whenever the WPA2 encryption keys are changed.

**COBIT 5: DSS06**

**ISO 27002: A.10**

**ISF SoGP: CF7, CF9**

## OS04 Audit WLAN access points.

**Control Objective**

To ensure WLAN access points are accessed by authorised personnel only.

**Control Description**

WLAN access points should include the following minimum set of events that should be audited:

1. Administration account logon and logoff success and failure.
2. Access point configuration changes.
3. Attempts to connect to access point management interfaces from unauthorised devices.
4. All WLAN authentication attempts, whether successful or not.

**COBIT 5: MEA02**

**ISO 27002: A.10, A.15**

**ISF SoGP: SI1**

| **OS05** | **Review log files.** |
|---|---|

**Control Objective**

To ensure that security events are recorded and identified.

**Control Description**

Authorised personnel should review log files on a regular basis to ensure that any signs of security violations are detected, and appropriate action is taken. Log files should be stored on alternate media, such as backup tapes, and should be retained for a minimum of 30 days. Additional auditing should be performed for interesting events, such as repeated WLAN probe requests for the broadcast SSID "ANY". Such events may indicate a malicious user searching for WLAN access points.

**COBIT 5: MEA02**

**ISO 27002: A.10**

**ISF SoGP: SI1, CF10**

| **OS06** | **Store WLAN access point firmware versions.** |
|---|---|

**Control Objective**

To promptly repair WLAN access points if a system failure were to occur.

| |
|---|
| **Control Description**<br>The WLAN access point firmware version and feature set that is installed should be stored in case of system failure, recovery or reconfiguration. |
| **COBIT 5: BAI10**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF9, CF14** |
| **OS07 Store WLAN information.** |
| **Control Objective**<br>To ensure WLAN information is easily accessible when needed. |
| **Control Description**<br>The WLAN access point serial numbers, hardware manufacturers, model names, vendor contact information and applicable warranty information should be stored in order to facilitate repairs. In addition, a list of all people with administrative privileges on the WLAN access points should be stored. |
| **COBIT 5: BAI10**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF6, CF9** |
| **OS08 Establish a data backup and recovery plan.** |

| |
|---|
| **Control Objective**<br>To ensure WLAN operations may be recovered speedily when errors occur. |
| **Control Description**<br>A data backup and recovery plan should be formulated for WLAN access points and related systems configurations so as to protect against configuration data loss. The backup and recovery process should be tested to ensure that it works in practice. |
| **COBIT 5: DSS04**<br>**ISO 27002: A.14**<br>**ISF SoGP: CF7, CF20** |

## 6.7 Using the WLAN Security Control Framework

This section describes a procedure for the implementation of the WLAN Security Control Framework by presenting the Plan-Do-Check-Act cycle, followed by a sample scenario.

### 6.7.1 Plan-Do-Check-Act

An organisation's management cycle typically consists of defining objectives and strategy, implementing operational plans, evaluating on going progress, enhancing performance and responding to both internal and external factors (ISO/IEC 27001, 2005).

The "Plan–Do–Check–Act" (PDCA) cycle is used by various organisations to implement quality management and the continuous improvement of information security management systems (ISO/IEC 27001, 2005). The PDCA cycle was identified as a suitable process that may be used for implementing WLAN security in SMMEs. In addition, it also meets the research objective of developing and implementing a WLAN security control framework for SMMEs. Figure 6.3 depicts the PDCA cycle which is discussed below.

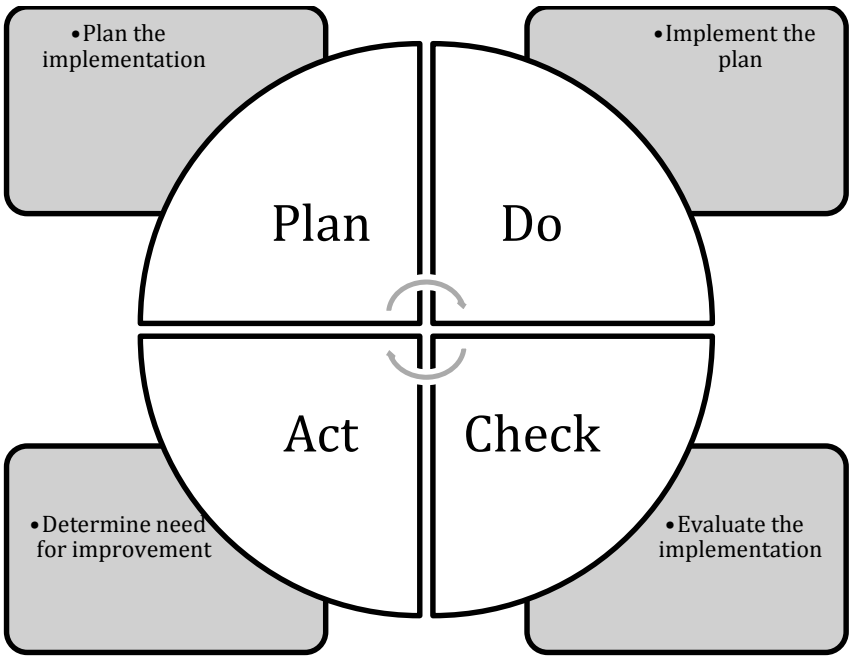



Figure 6.3: The PDCA Cycle (Redrawn and simplified from ISO/IEC 27001, 2005)

- Plan – The first step (plan stage) involves planning the implementation of the WLAN Security Control Framework by establishing the objectives and identifying the controls relevant to the organisation.
- Do – After the plan has been formulated, the next step (do stage) involves implementing the plan and executing the controls. It is during this step that an organisation should gain a sound understanding of the security environment.
- Check – The next step (check stage) involves evaluating the overall implementation of the controls and comparing them with the expected results.
- Act – During the next step (act stage), the implementation is concluded by determining which of the controls need to be improved.

The four steps of the PDCA cycle should be repeated continuously until there is no more need for improvement.

### 6.7.2 Example Scenario

A small legal firm in South Africa is concerned about security. The firm employs 6 staff members whose laptop computers are all connected wirelessly to the company network. The company has recently been experiencing a degradation in network performance and suspects that unauthorised persons are gaining access to the WLAN.

#### *6.7.2.1 Plan*

The intention of the legal firm is to find a solution for the degradation of the network performance and to identify the controls that are relevant to its problem.

According to the SMME classification presented in Table 4.2, this firm may be classified as a small enterprise (6–50 employees). When applying the WLAN Security Control Framework to the hacking problem mentioned above, the following controls are deemed to be relevant for a small enterprise, namely, TS01, TS02, TS03, TS04, TS05, TS06, TS07, TS08, TS10, TS15, TS18, OS04, and OS05. These were identified by scrutinising the control matrix presented in Table 6.7 and extracting the controls where there are ticks in both the “SMALL” and

"HACKING" columns. It would appear from the table that all of these controls are fundamental and, therefore, they must all be implemented. It may be noted that a control may mitigate more than just the "HACKING" threat. For example, TS01 will mitigate the "MISUSE" threat as well as the "HACKING" threat for small enterprises.

It is possibly recommended that micro sized businesses give the framework to their outsourced IT technician to use when installing a WLAN.

#### *6.7.2.2 Do*

The next step involves implementing the plan and executing the controls, in this case, TS01. In other words, TS01 would have been identified as a fundamental control which must be implemented in order to protect the legal firm against hacking. The control activity name for TS01 is "Secure the SSID". It is clear from Table 6.9 that the objective of this control is to ensure that WLANs meet the security requirements of the organisation in question and that authorised individuals only may gain access to the WLAN. It is also clear from reading the control description of TS01 in Table 6.9 that the default SSID supplied by a vendor is public knowledge and, thus, it constitutes a security risk for potential malicious users. Accordingly, it is imperative that it should be changed immediately when the WLAN is set up. If the legal firm wishes to read further about the background to this control it may refer to COBIT 5: DSS05, ISO 27002: A.10, and/or ISF SoGP: CF7 and CF9 as shown in the table under control TS01.

All the WLAN Security Control Framework controls identified in the plan stage may be implemented in this manner.

#### *6.7.2.3 Check*

The next step involves evaluating the implementation of the controls and ascertaining whether there has been an improvement in the performance of the firm's network.

#### *6.7.2.4 Act*

To conclude the implementation of the controls it is necessary in order to determine which of the controls need to be improved. Based on the outcome of this stage, it may be necessary to repeat the Plan-Do-Check-Act stages.

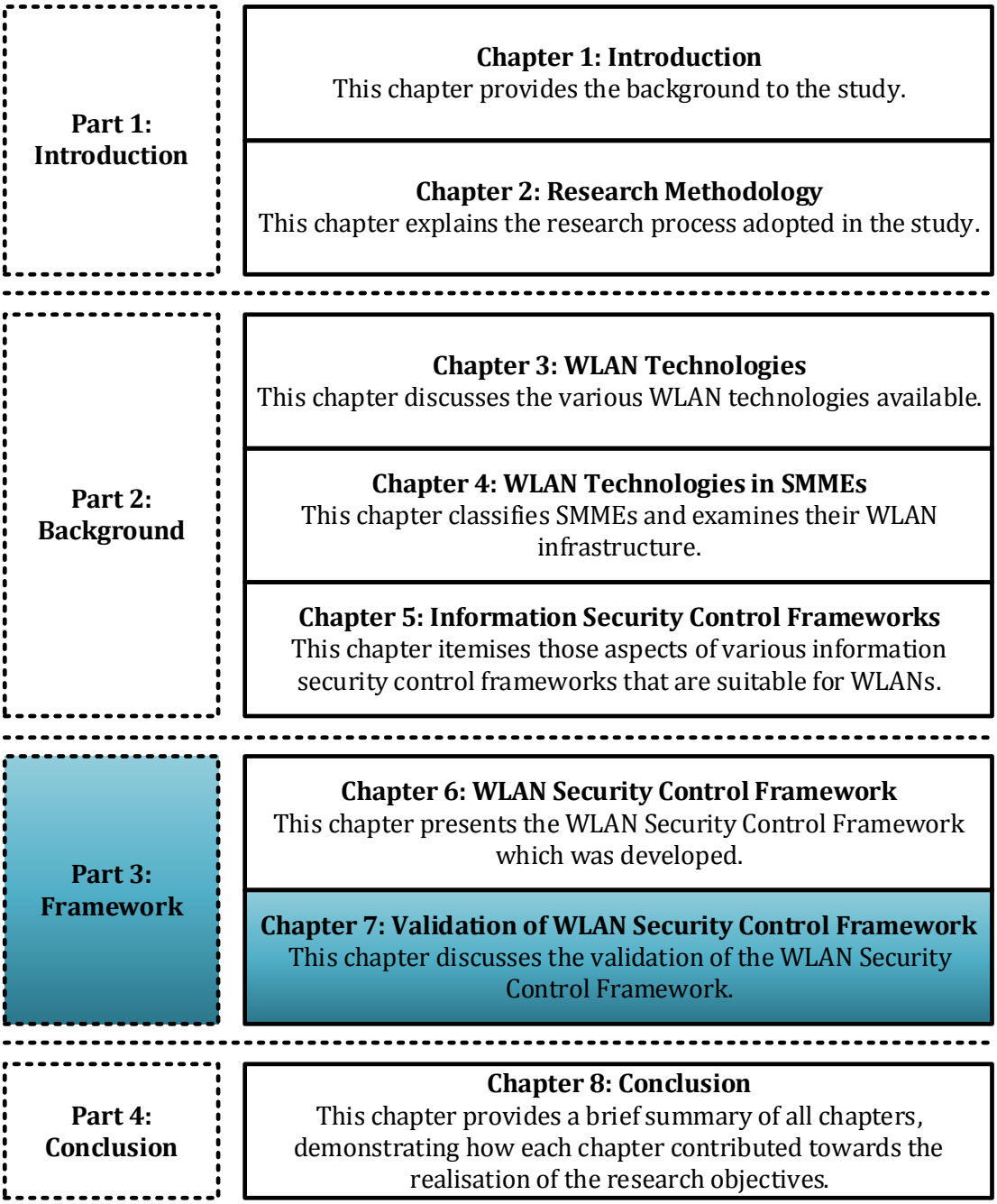
## 6.8 Conclusion

This chapter discussed the WLAN Security Control Framework for SMMEs.

The WLAN Security Control Framework was developed from a number of international standards, namely, COBIT 5 for Information Security (COBIT 5), ISO/IEC 27002:2005 (ISO 27002) and the ISF Standard of Good Practice 2012 (ISF SoGP). The contents of the framework were separated into three security areas, namely, physical security, technical security, and operational security. Each item in the framework was accompanied by controls that would assist in mitigating threats identified to SMMEs in South Africa. A process for using the framework was also proposed using the PDCA cycle with a sample scenario.

It is essential that the WLAN Security Control Framework be validated and, thus, this is the focus of the next chapter.

# 7 Validation of the WLAN Security Control Framework



## 7.1 Introduction

Chapter 6 presented the Wireless Local Area Network (WLAN) Security Control Framework for small, medium and micro sized enterprises. This chapter reports on the validation of the WLAN Security Control Framework. It was important to validate both the quality and the usability of the control framework in order to ensure its value. Section 2.2.4 discussed possible methods for the validation of the control framework. Section 7.2 suggests a focus group as a validation method while section 7.3 explains the development of the validation instrument. The composition of the focus group is discussed in section 7.4 and this is followed by the feedback of the focus group presented in section 7.5. Section 7.6 concludes the chapter.

## 7.2 The Focus Group as a Validation Method

In order to validate the WLAN Security Control Framework and as discussed in section 2.2.4, a focus group was conducted. A focus group was deemed to be useful for this validation exercise because it allowed multidisciplinary participants to interact without there being any pressure to reach agreement on the process. The multidisciplinary composition of the focus group enabled a broad range of responses which, in turn, enabled a number of different issues to be discussed. An instrument was created for use in the validation process. This instrument took the form of a questionnaire which was intended to collect qualitative data.

## 7.3 Creation of the Validation Instrument

In order to facilitate the validation process by means of a focus group, an instrument was developed. This instrument consisted of several statements relating to the WLAN Security Control Framework and invited the members of the focus group to comment on the statements. Before using the instrument, a presentation was delivered to the focus group. The presentation contained a brief overview of the framework and presented sample scenarios. The scenarios typically included various types of business and the related security risks. The framework was then applied to the scenarios and the focus group determine whether the framework presented appropriate solutions to the security problems.

The presentation and the scenarios as well as the instrument used in the validation process are contained in Appendix B.

## 7.4 Composition of the Focus Group

The focus group comprised ten people – eight participants and the researcher and the research supervisor. The researcher formally presented the framework and the scenarios but did not take part in the focus group discussion. The research supervisor was also present to act as a facilitator for any questions asked in order to ensure there was no bias. The eight members of the focus group were information technology (IT) professionals with the following experience:

- Doctoral students in IT Information Security
- Master's degree holders in IT Information Security and Networking
- Bachelor degree holders in IT Networking
- IT governance specialists
- Networking specialists (including wireless networks)
- Information security specialists

The aim of the focus group was to validate the WLAN Security Control Framework. Two scenarios were presented to the group together with the framework.

## 7.5 Overview of the Feedback

The members of the focus group were requested to indicate whether they agreed or disagreed with a number of statements. The range of answers included five options, namely, fully disagree, partially disagree, neutral, partially agree, and fully agree. There was also a space for the members to provide reasons for their choices regarding each statement.

Statement 1 referred to the members' qualifications, work experience, and job descriptions (summarised above).

*Statement 2: The framework is laid out logically and, therefore, it is easy to understand.*

All of the members either fully agreed or partially agreed with the statement. Accordingly, the researcher assumed that the WLAN Security Control Framework

is, in fact, logically laid out and easy to understand and that no further work was required in order to improve it.

*Statement 3: The way in which the framework is used is intuitive and, therefore, a small business owner would be able to use it.*

Six of the 8 focus group members either fully agreed or partially agreed with the statement while the remaining 2 were neutral. Three indicated that micro business users would require training in how to use the framework while one member also mentioned that smaller businesses may find that implementing the framework would take up too much time. The researcher took cognisance of the fact that it may involve too much work for small businesses to implement the framework. However, it is not possible to remove controls without introducing additional security risks into the environment. A recommendation from the focus group was that micro businesses give the framework to their outsourced IT technicians to use when installing a WLAN. This recommendation was, thus, added to the plan phase of the scenario as discussed in section 6.7.2.1 where procedures for the implementation for the framework are suggested.

*Statement 4: As regards Scenario 1 – a small legal firm with a hacking problem – the framework suggests sensible and appropriate security controls.*

Seven of the 8 focus group members either fully agreed or partially agreed with the statement while the remaining member was neutral. The latter had had no experience in personally implementing security controls and, thus, he/she was not in a position to comment. Accordingly, the researcher concluded that the framework serves its purpose.

*Statement 5: As regards Scenario 2 – a new micro business – the framework suggests sensible and appropriate security controls.*

Six of the eight members either fully agreed or partially agreed with the statement while the remaining members were neutral. It was mentioned again that smaller businesses may find the controls too technical in nature although it was agreed that the controls were appropriate. Accordingly, the researcher concluded that the framework serves its purpose.

In the extra comments that were provided there was a suggestion of a software programme or a toolbox for implementing the framework. Another comment indicated that an enterprise without an IT department would require additional explanations on implementing the controls. Section 6.7.2.2 suggested further reading on the background of the controls in the information security control framework standards.

## 7.6 Conclusion

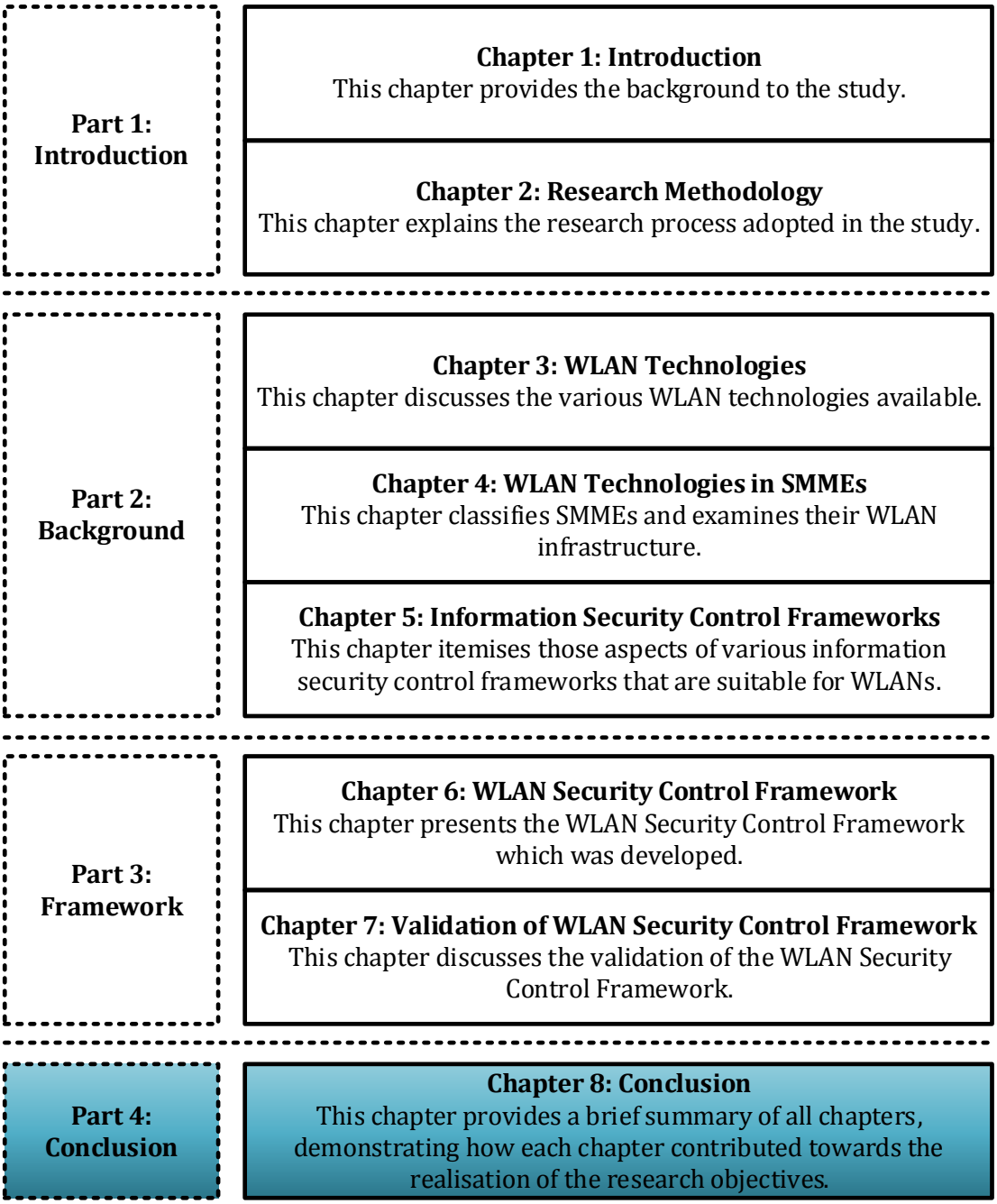
This chapter described the validation of the WLAN Security Control Framework which had been developed in order to ensure its quality.

The main aim of the focus group was to ascertain whether the research study has had contributed to addressing the gaps identified in current approaches for securing WLANs in small, medium, and micro enterprises (SMMEs) (see section 1.5).

At the end of the validation it was concluded that the WLAN Security Control Framework was logically set out, easy to use and that it recommended sensible and appropriate controls for the given scenarios and, thus, it was deemed to serve its purpose. The researcher does, however, take cognisance of the fact that certain small businesses may require training in the use of the framework.

Thus, the results from the focus group support the notion that this research study has contributed to addressing the gaps identified in current approaches for securing WLANs in SMMEs. It may, thus, be concluded that the WLAN Security Control Framework developed may be deemed to be valid.

# 8 Conclusion



## 8.1 Introduction

This chapter concludes the research study. Section 8.2 details the results of the study, section 8.3 summarises the contribution made by the study and section 8.4 discusses the limitations of the study. Section 8.5 contains suggestions for further research while section 8.6 concludes the study.

## 8.2 Results of the Research

As discussed in the study, information technology is important for modern businesses and brings numerous benefits by enabling communication and creating opportunities. This is especially true for small businesses which are now able to transact with larger organisations as a result of their ability to communicate electronically by means of networking.

In view of the reliance of businesses on their information and technology resources, it is important that these resources are protected to prevent any loss of business. Companies may use the international information security framework standards as discussed in this dissertation. However, these standards may not necessarily be appropriate for small, medium and micro enterprises (SMMEs) in South Africa. In fact, the researcher conducted a small survey to determine whether SMMEs in South Africa currently use WLANs and how these WLANs are protected. The details of this survey are contained in Appendix A.

It emerged from the survey that WLANs are used extensively by SMMEs but there is a lack of WLAN security controls. The latter was seen as a problem and led to this research endeavour.

The primary objective of this study was, therefore, to develop a framework that small, medium, and micro enterprises (SMMEs) may use to implement wireless local area network (WLAN) security. This framework, termed the WLAN Security Control Framework, was based on applicable security standards and best practices.

In order to achieve the primary research objective, it was necessary to realise the following sub-objectives. The procedure followed used to realise the primary research objective is also described below:

- Determine the needs of SMMEs with regard to WLAN security.
    - Chapter 3 examined WLAN technologies, threats, and security. It was identified that WLANs have different security requirements as compared to wired networks. The typical threats that face WLANs were identified and the security controls to mitigate these threats were discussed in terms of physical security, technical security, and operational security.
    - Chapter 4 began by classifying SMMEs in Table 4.2 and proceeded with a detailed discussion of the WLAN technologies that may be used by SMMEs. It was realised that WLANs were more suitable to SMMEs than wired networks. However, it was suggested that, as compared to larger organisations, SMMEs do not have the resources, knowledge, and skills required to secure WLANs effectively. Thus, for SMMEs to put effective WLAN security controls in place, a framework to assist them would be valuable.
- Investigate existing security control framework standards that govern WLANs.
    - Chapter 5 investigated a number of security control framework standards which may be used to govern an organisation's information security. The three frameworks identified as applicable to this research study included the following; Control Objectives for Information and Related Technology 5 for Information Security (COBIT 5), International Organisation for Standardisation and the International Electro-technical Commission 27002:2005 (ISO 27002), and Information Security Forum Standard of Good Practice 2012 (ISF SoGP). However, although these security frameworks included some network security controls, these were not specifically tailored for securing WLANs. However, it was decided that certain aspects of these security controls could be extracted and adapted for the purposes of securing WLANs.
- Determine the components that should form part of a WLAN Security Control Framework to support SMME needs in South Africa.

- It emerged from an examination of the three security control framework standards which were discussed in Chapter 5 that these frameworks were not entirely suitable for SMMEs as they were aimed at larger corporations and for experienced security professionals. SMMEs would not always have the security staff necessary to understand and implement these controls.
- An assessment was conducted of the information security control framework standards in that they were analysed for relevance to the research topic. This exercise was illustrated in Tables 6.1, 6.2, and 6.3.
- A number of controls from the security control framework standards were, therefore, extracted and listed based on their relevance to the securing of WLAN implementations in SMMEs. Tables 6.4, 6.5, and 6.6 depict the controls extracted.
- Using all the information collected, new controls for the WLAN Security Control Framework were designed and presented in a control matrix as depicted in Table 6.7. The detailed contents of the framework was classified under three security areas, namely, physical security, technical security, and operational security – See Tables 6.8, 6.9, and 6.10 respectively. The framework presented security controls that would assist in mitigating the WLAN threats identified to SMMEs in South Africa.

The realisation of the sub-objectives discussed above and subsequent validation process meant that the primary research objective of this study was achieved.

## 8.3 Contribution of the Research Study

Regarding the significance of the research study, it was found that the international security control framework standards were not suitable for the securing of WLANs in SMMEs. This is primarily as a result of the fact that these standards are tailored for larger organisations with expert security staff and the considerable resources required to implement the controls. The primary contribution of this research study is, therefore, the WLAN Security Control Framework for SMMEs in South Africa. The implementation of this framework will

help SMMEs improve the state of their WLAN security by providing them with protection against the escalating threats of malware, hacking, social engineering, misuse, physical threats, error threats and environmental threats. A research paper presenting this framework was prepared and will be submitted to a relevant subject specific journal. The draft paper is contained in Appendix C.

## 8.4 Limitations of the Research

In view of time and resource constraints on the part of the researcher the WLAN Security Control Framework has not been tested in real-world situations. It was, however, validated by means of a focus group and using sample scenarios. Nevertheless, the researcher acknowledges that this is a weakness and that further validations should take place to ensure the effective implementation of the framework for WLANs in SMMEs.

## 8.5 Suggestions for Further Research

There are a number of areas in which further research may be conducted. It would be beneficial if the WLAN Security Control Framework were to be implemented in an SMME to ensure that the framework covers all the possible WLAN security threats. It would also benefit SMMEs if an implementation guide were developed to assist them. In addition, another security control framework for SMMEs for end-to-end security would also be useful. For larger organisations a more detailed WLAN Security Control Framework would be required.

## 8.6 Conclusion

Small, medium and micro enterprises play a vital role in the South African economy. These companies are becoming increasingly reliant on WLANs to provide business communication. It is, therefore, vital to assist these enterprises with the protection of their WLAN infrastructure. The researcher hopes that this dissertation will help in providing assistance to SMMEs and also encourage other researchers to contribute to this topic.

# 9 References


Abor, J., & Quartey, P. (2010). Issues in SME Development in Ghana and South Africa. *International Research Journal of Finance and Economics*.

Babbie, E. R. (2005). *The basics of social research* (3rd ed.). Belmont: Wadsworth Publishing.

Baumann, R. (2002). Securing Wireless Local Area Networks (WLAN).

Bhargava, V., & Sichitiu, M. L. (2005). Physical Authentication through Localization in Wireless Local Area Networks. *Global Telecommunications Conference.* St Louis.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices.* Zurich: Global Text Project.

Carson, D., Gilmore, A., Perry, C., & Gronhaug, K. (2001). Qualitative marketing research. SAGE publications.

Chandra, P., Bensky, A., Bradley, T., Hurley, C., Rackley, S., Rittinghouse, J., . . . Wilson, J. (2009). *Wireless Security: Know It All.* Oxford: Newnes.

Chen, S. Y., Katsaros, D., Nanopoulos, A., & Manolopoulos, Y. (2005). *Wireless Information Highways.* Hershey: IRM Press.

Cisco Systems, Inc. (2003). *2003 Wireless LAN Benefits Study.* San Jose: NOP World Technology.

Eldad, P., & Stacey, R. (2013). *Next Generation Wireless LANs: 802.11n and 802.11ac.* Cambridge University Press.

European Commission. (2003). The New SME Definition. *Official Journal of the European Union*.

Fuller, T. (2003). If you wanted to know the future of small business what questions would you ask? *Futures*.

Gillham, B. (2000). *The research interview.* London: Continuum.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quartely, 28*(1), 75-105.

Hochschild, J. (2009). *Workshop on Interdisciplinary Standards for Qualitative Research*. Retrieved from Harvard Scholar: http://scholar.harvard.edu/jlhochschild/publications/conducting-intensive-interviews-and-elite-interviews

*IEEE 802.11n-2009.* (n.d.). Retrieved July 23, 2011, from IEEE Computer Society: http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

Information Security Forum. (2012). *The Standard of Good Practice for Information Security.* Information Security Forum Limited.

ISACA. (2012). *COBIT 5 for Information Security.* Rolling Meadows.

ISO/IEC 27001. (2005). *ISO/IEC 27001 Information technology - Security techniques - Information security management systems - requirements.* Geneva.

ISO/IEC 27002. (2005). *ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management.* Geneva.

Krippendorff, K. (2004). *Content analysis: an introduction to its methodology* (2nd ed.). Thousand Oaks: Sage Publication.

Krueger, R., & Casey, M. (2000). *Focus groups: A practical guide for applied researchers* (3rd ed.). Thousand Oaks: Sage.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research: Planning and design* (7th ed.). New Jersey: Prentice Hall.

Lester, S. (1999). *An introduction to phenomenological research.* Taunton: Stan Lester Developments. Retrieved from http://www.sld.demon.co.uk/resmethy.pdf

Levy, J., Tran, K., Lydon, P., Pollock, J., Parry, D., & Weigand, S. (2008). *SonicWALL Secure Wireless Network Integrated Solutions Guide.* Burlington: Sungress Publishing, Inc.

Lewis, B., & Davis, P. T. (2004). *Wireless Networks for Dummies.* Hoboken: Wiley Publishing Inc.

Marshall, C., & Rossman, G. (2011). *Designing qualitative research* (5th ed.). SAGE Publications.

Mason, J. (2002). *Qualitative researching* (2nd ed.). London: SAGE Publications.

McCullough, A. (2001). *Designing a wireless network.* Syngress Pub.

Mitra, S. (2005). Information technology as an enabler of growth in firms: An empirical assessment. *Journal of Management Information Systems, 22*(2), 279-300.

Mouton, J. (2001). *How to succeed in your Master's & Doctoral Studies.* Pretoria: Van Schaik Publishers.

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly, 21*(2), 241-242.

NIST. (2006). *NIST Special Publication 800-100: Information Security Handbook A Guide for Managers.* Gaithersburg: National Institute of Standards and Technology.

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

Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. *European Journal of Information Systems, 15*(2), 120-131.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.

Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: the role of human, business, and technology resources. *Strategic management journal, 18*(5), 375-405.

Rackley, S. (2011). *Wireless Networking Technology: From Principles to Successful Implementation.* Oxford: Elsevier.

Sanders, A. (2011). *What is Network Infrastructure?* Retrieved April 20, 2011, from wiseGEEK: http://www.wisegeek.com/what-is-network-infrastructure.htm

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students* (3rd ed.). Prentice Hall.

*Small Business Administration*. (2011). Retrieved June 6, 2011, from SBA.gov: http://www.sba.gov/about-sba

*South Africa.* (1996). Retrieved June 6, 2011, from No. 102 of 1996: National Small Business Act: http://www.info.gov.za/acts/1996/a102-96.pdf

*South Africa.* (2003). Retrieved June 6, 2011, from No. 26 of 2003: National Small Business Amendmant Act: http://www.info.gov.za/view/DownloadFileAction?id=68002

Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *Political Science and Politics, 40*(4).

Tapia, I. M., Correa, J. A., & Manzanares, A. R. (2009). Environmental Strategy and Exports in Medium, Small and Micro-Enterprises. *Journal of World Business*.

Tapscott, D., & Caston, A. (1993). *Paradigm Shift: The New Promise of Information Technology.* New York: McGraw Hill, Inc.

Upfold, C. T., & Sewry, D. A. (2005). An Investigation of Information Security in Small and Medium Enterprises (SME's). *Information Security South Africa.* Sandton.

Vaishnavi, V., & Kuechler, W. (2004). *Design Research in Information Systems.* Retrieved October 10, 2014, from http://desrist.org/design-research-in-information-systems/

Von Bon, J. (2007). *IT Service Management Based on ITIL V3: A Pocket Guide.* Zeltbommel: Van Haren Publishing.

Wilkinson, S. (2004). *Qualitative research: Theory, method & practice* (D. Silverman ed.). Thousand Oaks: SAGE.

Wilson, M., & Hash, J. (n.d.). *Information Technology Security Awareness, Training, Education, and Certification*. Retrieved April 23, 2011, from NIST Information Technology Laboratory: http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm

Wong, A., & Yeung, A. (2009). *Network Infrastructure Security.* New York: Springer.

# 10 Appendices

Several documents have been included as appendices for additional information purposes. The documents include the following:

1. Appendix A: Survey Results
2. Appendix B: Focus Group Validation Presentation and Instruments
3. Appendix C: Draft Journal Paper

## 10.1 Appendix A: Survey Results

There is not much literature available that is specific to the use of WLAN security amongst small, medium and micro enterprises (SMMEs) in South Africa. Accordingly, the researcher conducted a survey to determine whether there was a need for a WLAN Security Control Framework aimed specifically at securing WLANs in SMMEs.

The South African SMME population is so large that a sample group was chosen and the findings generalised to the entire population of SMME's.

A pilot study was first conducted on a small group of the population. This was done in order to identify problems in the survey (e.g. misunderstood questions, unexpected responses).

The survey data was collected using a web survey tool provided by the Nelson Mandela Metropolitan University. The survey was posted as a link on various SMME forums and sent by email to various companies (http://www.nmmu.ac.za/websurvey/q.asp?sid=310&k=hsoiusptdm).

A total of 64 companies participated in the survey, including micro, small, medium and large enterprises. The data received from these companies was then analysed with the expectation that each question would have different outcomes because the respondents had answered from a departmental, divisional or organisational viewpoint. In some cases the respondents were clearly unaware of the answer to the question and had probably guessed.

Every member from within an organisation – from a human resource employee to an IT administrator –- had an equal chance of being included in the sample. Accordingly, the sample was selected randomly. Employees from all departments in various organisations had participated in the survey as SMMEs do not always have a dedicated IT department. This, in turn, implies that all the data collected did not give preference to any particular members of the population. Employees of the companies were asked for their opinions in order to ascertain whether they were aware of WLAN security.

The questions in the survey were intended to find out how many people were employed in the companies as this would indicate whether the companies were

micro, small, medium or large in size. The companies also indicated whether they made use of a WLAN and whether they had adequate WLAN security in place. Two types of measurements were used when designing the questions, namely, nominal measurements and ratio measurements. In addition to choosing these measurements, closed questions were used, thus restricting the respondent to selecting a specific answer from a list of possible answers.

The data was gathered online using the web survey tool mentioned earlier. This tool collected the data in a spreadsheet format. The answers in the columns of the spreadsheet were added together and the totals were analysed. The totals collected were then expressed in graphical format using pie charts and bar graphs. This was done by taking the total number of small, medium or micro sized businesses and calculating the percentages of people who had answered either yes or no in the survey.

The questions are listed below:

***Question 1: How many people are employed in your company?***

As shown in Figure 10.1 the results obtained were grouped to show the different types of enterprises.

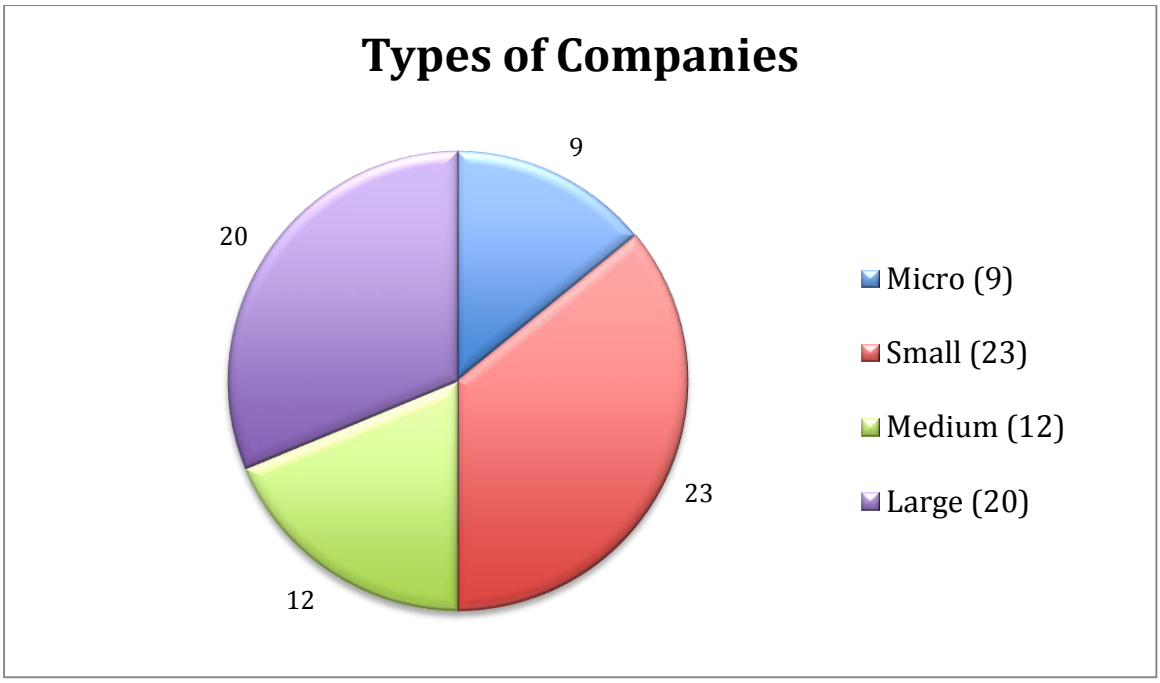



Figure 10.1: Types of Companies Surveyed.

Of the sixty-four (64) companies that participated in the survey:

- 9 were micro enterprises (less than 5 employees);
- 23 were small enterprises (less than 50 employees);
- 12 were medium enterprises (less than 200 employees);
- 20 were large enterprises (more than 200 employees).

These results provided an indication of the types of enterprises that had participated in the survey. This information was then used to ensure that the interpretations of the results are, in fact, applicable to SMMEs.

***Question 2: Does your company make use of a WLAN?***

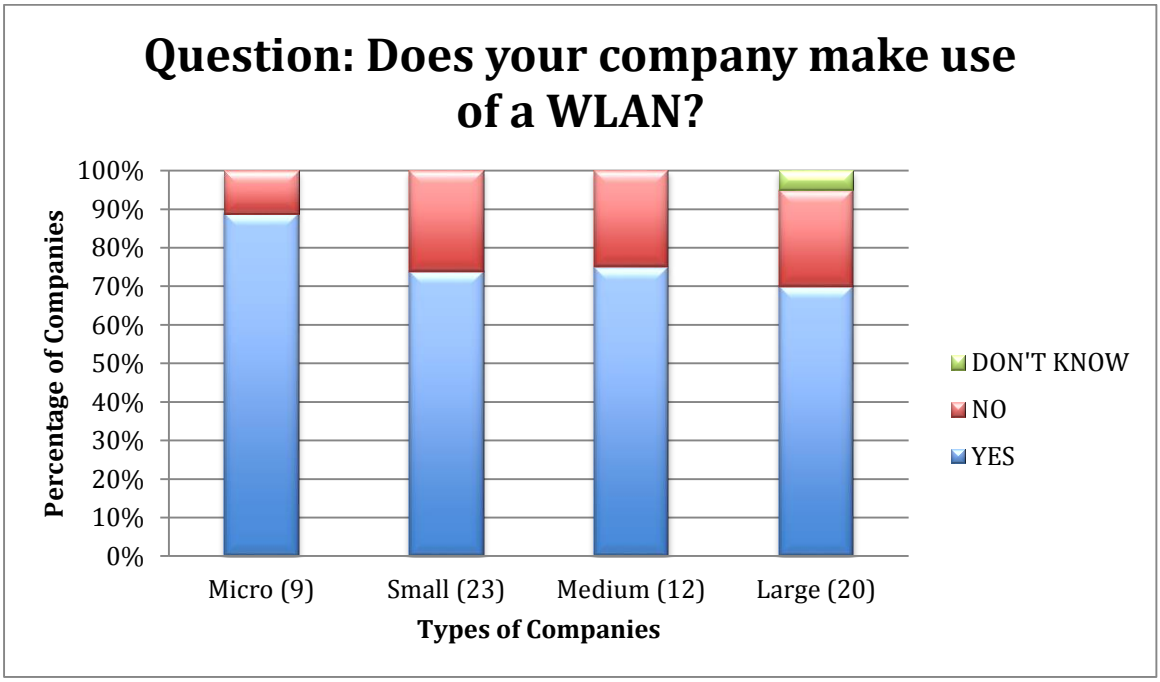



Figure 10.2: Percentage of Companies Surveyed that had WLANs.

- 88% of micro enterprises made use of WLANs;
- 72% of small enterprises made use of WLANs;
- 73% of medium enterprises made use of WLANs;
- 70% of large enterprises made use of WLANs.

A total of 77% of the SMMEs that participated in the survey made use of WLANs. Thus, ensuring the security of such WLANs would be of importance to most SMME's.

***Question 3: Does your company have adequate WLAN security?***

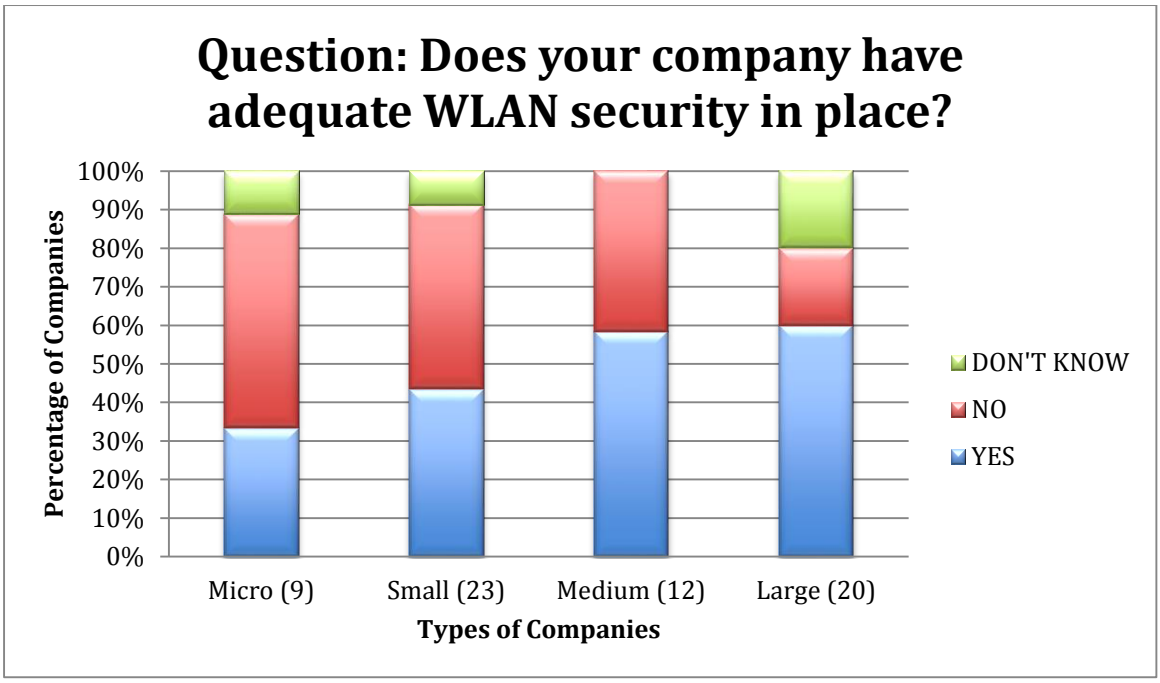



Figure 10.3: Percentage of Companies that have Adequate WLAN Security.

- 31% of micro enterprises had adequate WLAN security;
- 41% of small enterprises had adequate WLAN security;
- 58% of medium enterprises had adequate WLAN security;
- 59% of large enterprises had adequate WLAN security.

This reveals that that 71% of the SMMEs that had WLANs did not have adequate WLAN security or that the employees were unaware of the type of WLAN security controls that existed in their organisation. This lack of WLAN security, in combination with the fact that 77% of the SMMEs surveyed used WLANs, clearly showed that there was a need for WLAN security amongst SMMEs.

***Question 5: Do you think there is a need for better WLAN security in your company?***

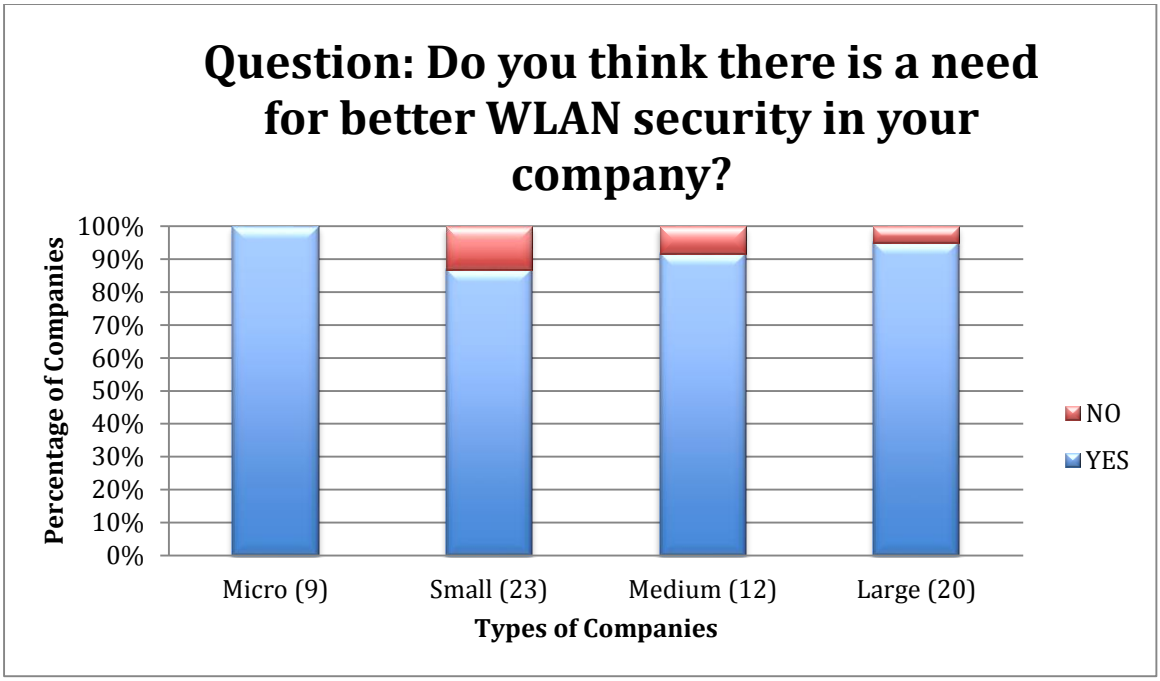
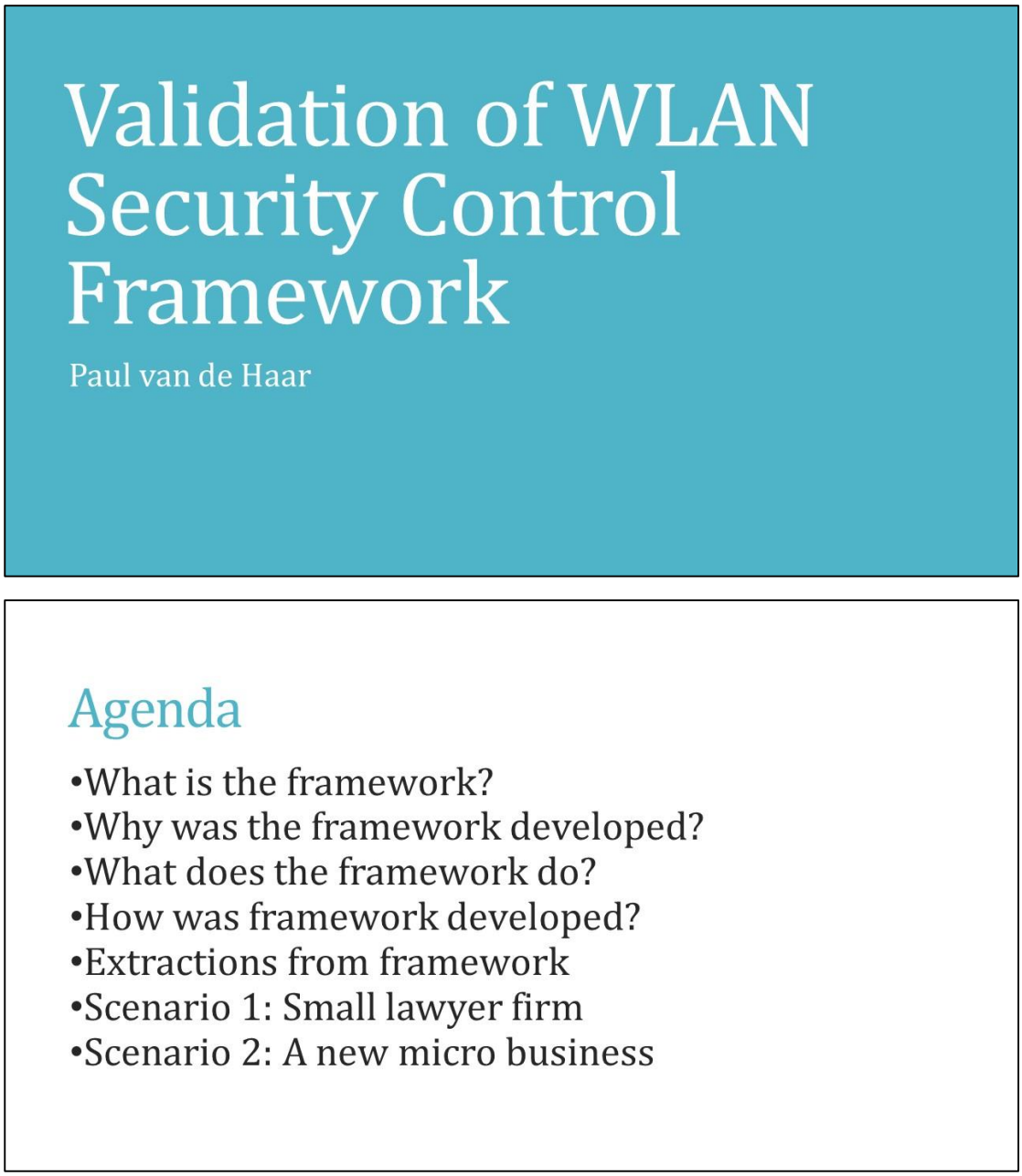



Figure 10.4: Percentage of Companies that think there is a Need for Better WLAN Security within their Company.

- 100% of micro enterprises indicated there was a need for better WLAN security;
- 87% of small enterprises indicated there was a need for better WLAN security;
- 92% of medium enterprises indicated there was a need for better WLAN security;
- 95% of large enterprises indicated there was a need for better WLAN security.

Figure 10.4 shows that a total of 91% of the SMMEs that participated in the survey had indicated that there was a need for better WLAN security controls in their companies.

## 10.2 Appendix B: Focus Group Validation Presentation and Instrument



## What is the framework?

The WLAN Security Control Framework is a framework used to improve the WLAN security state of SMME's.

## Why was the framework developed?

Current information security control frameworks not created with SMME's in mind:

- They are exhaustive and aimed at large corporations
- Not freely available, requiring extensive resources to purchase
- Controls are aimed at experienced security professionals
- Too complex for ordinary SMME staff
- Not specifically related to securing WLANs

## What does the framework do?

Helps SMME's to secure their WLANs against the escalating threats of:

- Malware
- Hacking
- Social engineering
- Misuse
- Physical threats
- Error threats
- Environmental threats

## How was framework developed?

1. Identified requirements for WLAN security
2. Identified requirements for SMME's
3. Researched information security control frameworks (COBIT 5, ISO 27002, ISF SoGP)
4. Extracted controls relevant to securing WLANs in SMME's
5. Designed new controls classified under Physical Security, Technical Security, and Operational Security.

# Extractions from framework

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| **PHYSICAL SECURITY** | | | | | | | | | | | | |
| PS01 | Secure antennas and related cabling supporting WLANs. | F | | | ✓ | | ✓ | | | ✓ | | ✓ |
| PS02 | Secure WLAN access points. | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS03 | Secure WLAN client devices. | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS04 | Train staff on the general risks of WLANs. | F | | ✓ | ✓ | | | ✓ | | ✓ | | ✓ |
| PS05 | Control access to secure areas. | S | | | ✓ | | | ✓ | | ✓ | | ✓ |

## PHYSICAL SECURITY

**PS01 Secure antennas and related cabling supporting WLANs.**

**Control Objective**

To protect antennas and related cabling that support WLANs from interception or damage.

**Control Description**

Antennas and related cabling that is supporting the WLANs should be kept in a secure area where access is restricted to authorized personnel. Suitable physical access controls should be in place where WLAN access points are located. The following WLAN security activities should be implemented:

1. Attach identification labels to antennas and cables.
2. Conceal the installation of antennas and cables.
3. Avoid routing cables through publicly accessible areas.
4. Document diagrams to show where antennas and cables are located.

**COBIT 5: DSS05**

**ISO 27002: A.9**

**ISF SoGP: CF9, CF19**

**PS02 Secure WLAN access points.**

**Control Objective**

To prevent unauthorised users or malicious users from physically gaining access to WLAN access points.

**Control Description**

WLAN access points should be kept in a secured closet or enclosure where access is restricted to authorized personnel. Malicious users that gain physical access to a WLAN access point are able to bypass all network security measures. Organisations should make sure that these WLAN access points are not located in common areas, such as kitchens, canteens, or open offices. The following WLAN security activities should be implemented:

1. Position the WLAN access points in secure environments (e.g. Locked rooms or cabinets).
2. Document diagrams to show where WLAN access points are located.

**COBIT 5: DSS05**

**ISO 27002: A.9**

**ISF SoGP: CF9, CF19**

# Scenario 1: Small lawyer firm

A lawyer firm in South Africa is concerned about security:

- 6 staff members with laptops connected to WLAN (classified as small according to research)
- Experiencing degradation in WLAN performance
- Suspect unauthorised persons have access to WLAN (hacking threat)

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| PS08 | Deploy redundant WLAN access points. | F | | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS09 | Secure backups. | F | | | ✓ | | | | ✓ | ✓ | ✓ | ✓ |
| PS10 | Protect WLAN access points with UPS. | F | | | ✓ | | | | | | ✓ | ✓ |
| TECHNICAL SECURITY | | | | | | | | | | | | |
| TS01 | Secure the SSID. | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | |
| TS02 | Configure authentication. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS03 | Configure MAC address filtering. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS04 | Secure default WLAN access point settings. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS05 | Require a valid password prior to administrator access. | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | ✓ | |
| TS06 | Configure user accounts. | F | | ✓ | ✓ | | ✓ | | ✓ | | | |

| TS01 | Secure the SSID. |
|---|---|
| **Control Objective** | To ensure WLANs meet the security requirements of the organisation and only authorised individuals gain access to the wireless network. |
| **Control Description** | The SSID used to identify a WLAN should be changed from the vendor default. Although the task to discover an SSID is trivial, default SSIDs are often an indication that a WLAN has not been secured and may be enticement for the curious to investigate. These SSIDs should not provide potentially useful information to malicious users. Do not set SSIDs as values such as an organisation's name, address, floor or department because it may provide for an attractive target for potential intruders. |
| COBIT 5: DSS05<br>ISO 27002: A.10<br>ISF SoGP: CF7, CF9 | |

# Scenario 2: A new micro business

An entrepreneur has started a business at home:

- She purchased a WLAN device to connect to the internet.
- She wants to secure the WLAN and needs some guidance.
- She has limited resources and no knowledge of best practice for security.
- (classified as micro according to research)

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| **PHYSICAL SECURITY** | | | | | | | | | | | | |
| PS01 | Secure antennas and related cabling supporting WLANs. | F | | | ✓ | | ✓ | | | ✓ | | ✓ |
| PS02 | Secure WLAN access points. | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS03 | Secure WLAN client devices. | F | ✓ | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS04 | Train staff on the general risks of WLANs. | F | | ✓ | ✓ | | | ✓ | | ✓ | | ✓ |
| PS05 | Control access to secure areas. | S | | | ✓ | | | ✓ | | ✓ | | ✓ |
| PS06 | Conduct regular WLAN site surveys. | S | | | ✓ | | ✓ | ✓ | | | | |
| PS07 | Secure antennas as to minimize coverage. | F | | | ✓ | | ✓ | | | | | |

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| PS08 | Deploy redundant WLAN access points. | F | | ✓ | ✓ | | | | | ✓ | | ✓ |
| PS09 | Secure backups. | F | | | ✓ | | | | ✓ | ✓ | ✓ | ✓ |
| PS10 | Protect WLAN access points with UPS. | F | | | ✓ | | | | | | ✓ | ✓ |
| **TECHNICAL SECURITY** | | | | | | | | | | | | |
| TS01 | Secure the SSID. | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | |
| TS02 | Configure authentication. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS03 | Configure MAC address filtering. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS04 | Secure default WLAN access point settings. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |
| TS05 | Require a valid password prior to administrator access. | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | ✓ | |
| TS06 | Configure user accounts. | F | | ✓ | ✓ | | ✓ | | ✓ | | | |

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| TS07 | Disable unused and dormant user accounts. | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| TS08 | Configure strong passwords. | F | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | |
| TS09 | Disable responses to broadcast SSID probe. | S | | | ✓ | | ✓ | | | | | |
| TS10 | Perform user identification. | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| TS11 | Segregate WLANs from internal network. | F | | | ✓ | ✓ | ✓ | | | | | |
| TS12 | Secure gateways prior to accessing the internal network. | F | | | ✓ | ✓ | ✓ | | | | | |
| TS13 | Secure management interface on WLAN access points. | F | | | ✓ | | ✓ | | ✓ | | | |
| TS14 | Secure SNMP. | F | | | ✓ | | ✓ | | ✓ | | | |
| TS15 | Enable WPA2 encryption. | F | ✓ | ✓ | ✓ | | ✓ | | | | | |

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| TS16 | Encrypt WLAN devices. | F | | | ✓ | | ✓ | | | ✓ | | |
| TS17 | Encrypt data using high level protocols. | F | | | ✓ | | ✓ | | | | | |
| TS18 | Update WLAN device firmware. | F | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | |
| **OPERATIONAL SECURITY** | | | | | | | | | | | | |
| OS01 | Direct and monitor the WLAN Security Control Framework. | F | | ✓ | ✓ | | | | ✓ | | | |
| OS02 | Document a WLAN Security Policy. | F | ✓ | ✓ | ✓ | | | | ✓ | | | |
| OS03 | Distribute WPA2 encryption keys when changed. | F | ✓ | ✓ | ✓ | | | | | | ✓ | |
| OS04 | Audit WLAN access points. | F | | ✓ | ✓ | | ✓ | | ✓ | | | |
| OS05 | Review log files. | F | | ✓ | ✓ | | ✓ | | ✓ | | ✓ | |
| OS06 | Store WLAN access point firmware versions. | F | | | ✓ | | | | | | ✓ | |

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| OS07 | Store WLAN information. | F | | | ✓ | | | | | | ✓ | |
| OS08 | Establish a data backup and recovery plan. | F | | | ✓ | | | | ✓ | | ✓ | ✓ |

# Validation of WLAN Security Control Framework

**Introduction and aim of research study**

The aim of this research study was to develop a Wireless Local Area Network (WLAN) Security Control Framework for small, medium and micro sized enterprises (SMMEs) in South Africa.

**Questions:**

1. Please provide a description of your qualifications, work experience and job descriptions regarding WLANs and/or information security.

| |
|---|
| |

2. The framework is laid out logically and, therefore, easy to understand. Please motivate.

| Fully disagree | Partially disagree | Neutral | Partially agree | Fully agree |
|---|---|---|---|---|
| | | | | |

Motivation:

| |
|---|
| |

3. The way in which the framework is used is intuitive and, therefore, a small business owner will be able to use it. Please motivate.

| Fully disagree | Partially disagree | Neutral | Partially agree | Fully agree |
|---|---|---|---|---|
| | | | | |

Motivation:

| |
|---|
| |

4. For Scenario 1, which was a small legal firm with a hacking problem, sensible and appropriate security controls were suggested. Please motivate.

| Fully disagree | Partially disagree | Neutral | Partially agree | Fully agree |
|---|---|---|---|---|
| | | | | |

Motivation:

| |
|---|
| |

5. For Scenario 2, which was a new micro business, sensible and appropriate security controls were suggested. Please motivate.

| Fully disagree | Partially disagree | Neutral | Partially agree | Fully agree |
|---|---|---|---|---|
| | | | | |

Motivation:

| |
|---|
| |

6. Any other comments?

| |
|---|
| |

Thank you for your time.

## 10.3 Appendix C: Draft Journal Paper

# A FRAMEWORK FOR WIRELESS SECURITY IN SMMEs

P. VAN DE HAAR, J. VAN NIEKERK

## ABSTRACT

Many small, medium and micro enterprises (SMMEs) are relying on wireless local area networks (WLANs) for communication with customers, suppliers and other businesses. All organisations need to protect their information and infrastructure but there is not much literature available that is specific to the use of WLAN) security amongst SMMEs in South Africa.

This research paper seeks to provide assistance to SMMEs for securing their WLANs. The research process followed a design science approach in order to produce a solution. Literature studies were done on security control framework standards and WLAN technologies. The needs of SMMEs regarding WLANs were also established.

The result of the research process as described in this paper was an artefact in the form of a WLAN Security Control Framework for securing WLANs for SMMEs in South Africa.

**Keywords**: Framework, WLANs, SMMEs, Information Security

## 1. INTRODUCTION

Information technology (IT) is important for modern businesses in the information age where information and its' uses permeate modern life. IT is required to store, control, and manipulate a company's information bringing many benefits. A negative impact would result if IT functions were not suitably implemented. IT enables communication and creates opportunities, especially for small businesses who are now able to transact with larger organisations due to their ability to communicate electronically (Tapscott & Caston, 1993) (Powell & Dent-Micallef, 1997).

Modern businesses cannot compete unless they have access to information technology resources and specifically networking resources (Powell & Dent-Micallef, 1997). This is especially true for SMMEs because they have no major information technology divisions in their companies to support high availability requirements. SMMEs often use WLANs which brings its' own set of problems. Organisations, both big and small, need to protect themselves against increasing threats that are exacerbated by Internet communications (Upfold & Sewry, 2005).

There exists some guidance in the form of international information security best practice control framework standards. However, SMMEs do not necessarily have the financial resources available to purchase these standards and these standards are not *specific* to WLANs and more specifically the WLAN needs of SMMEs. Thus these standards are not necessarily useful in the context of securing WLANs within SMMEs. SMMEs require guidance that is less complex and require fewer resources to implement. Some of these IT security framework standards that companies can use are listed below:

- Control Objectives for Information and Related Technology (COBIT) 5 for Information Security (ISACA, 2012),
- International Organisation for Standardization and the International Electro-technical Commission (ISO/IEC) 27002:2005 (ISO/IEC 27002, 2005),
- Information Security Forum (ISF) Standard of Good Practice 2012 (Information Security Forum, 2012),
- Information Technology Infrastructure Library (ITIL) (Von Bon, 2007), and
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100 (NIST, 2006).

The next section describes the research methodology used for the artefact presented in this paper.

## 2. METHODOLOGY

The research process followed a Design Science methodology, using induction to collect information for developing a framework. Qualitative data was collected by means of literature reviews, observations and experience. The framework was validated using a focus group.

For the purpose of this research **design science** was chosen as the overarching philosophical paradigm. Design science is about developing something, in this case a WLAN Security Control Framework (Vaishnavi & Kuechler, 2004).

This research used **inductive** reasoning, which means that the information was collected and the framework was developed as a result. Further induction was applied when the framework was validated.

**Qualitative research** suited this particular research topic because the sources of data were mostly textual. Information was also collected through experience and theoretical knowledge of the researcher. Qualitative content analyses were conducted. The researcher would have remained objective when doing this qualitative research to build the framework (Bhattacherjee, 2012) (Myers, 1997) (Olivier, 2009).

Rigour research arguments were prepared in adherence to guidelines presented by Mason (2002) for evidential or interpretive arguments. The framework that was developed contained concepts, theories and expectations to support and inform SMMEs about securing WLANs. The contents of the framework were as a result of the data collection techniques as well as the researcher's knowledge, experiences and observation of SMMEs (Krippendorff, 2004).

In order to validate the framework, the research study adopted a **focus group** method. This allowed a multi-disciplinary validation in order to satisfy the requirements for information security knowledge, networking knowledge, and general research experience.

The next section describes some of the information gained during the literature reviews.

# 3. LITERATURE REVIEW

## 3.1 WLAN Technologies

Every business has information that is of strategic importance and also has a requirement to communicate with customers, suppliers, and other businesses. Information technology (IT), and networks in particular, are therefore important enablers. IT networks provides the facility for borderless communication and brings businesses closer together removing the distance barriers (Tapscott & Caston, 1993).

There are many types of IT networks that businesses may use. Local area networks (LANs) are usually a group of computers connected together in the same building. Computers in wide area networks (WANs) may be further apart and connected by telephone lines or radio waves because of the far distances. There are other types of networks in-between LANs and WANs such as campus area networks (CANs), and metropolitan area networks (MANs) (Baumann, 2002).

All of these IT networks can be built using either wired or wireless technologies. This research study focused on wireless local area networks (WLANs).

In 1997, the Institute of Electrical and Electronic Engineers (IEEE) developed a set of standards required for implementing WLAN communication between computers and pre-existing networks, including home and office networks, and the Internet. In the decade and a half since its release, WLANs have matured and grown immensely in capability, changing the face of computing, and communication in the world at large. However, WLANs have also become a large, confusing list of standards, tethered to the past by necessary backwards compatibility (Rackley, 2011).

WLANs bring specific information security related responsibilities. This section will discuss the various threats that are facing WLANs (Information Security Forum, 2012).

- **Malware threats** - The threat of malware to a WLAN is caused by malicious software, which has been developed for the purpose of compromising information and harming WLAN devices.
- **Hacking threats** - The threats of WLANs being hacked involve unauthorised external individuals deliberately attempting to access or harm an organisation's network by exploiting vulnerabilities and bypassing security controls.
- **Social engineering threats** - The threat of social engineering involves the use of social tactics to exploit an individual and influence them in performing specific actions such as disclosing WLAN authentication information.
- **Misuse threats** - The threat of misuse involves the unauthorised use of resources and privileges to gain access to information on a WLAN.
- **Physical threats** - Physical threats are typically associated with the loss or theft of WLAN equipment.
- **Error threats** - Error threats to WLANs are usually the result of mistakes made by one or more individuals.

- **Environmental threats** - Environmental threats are typically associated with WLANs being affected by natural events, such as floods or storms, or man-made events, such as fires, explosions, riots or electrical interference.

The three main goals of WLAN security are to protect an organisation from the loss of confidentiality, the loss of integrity and the loss of availability. Most security practices and controls can be traced back to protecting against the losses in one or more of these areas. These areas are often referred to as the CIA triad and they are the core principles of information security (ISO/IEC 27002, 2005):

- Confidentiality ensures that WLAN data is not disclosed to unauthorised users.
- Integrity ensures that WLAN data is correct and current.
- Availability ensures that WLAN devices and data are available when needed.

Organisation's should be aware that any flaws when protecting against the loss of CIA can be exploited for malicious purposes, so when organisation's secure their WLANs they need to consider three different types of security. These are physical security, technical security and operational security (Wong & Yeung, 2009).

## 3.2 WLAN Technologies in SMMEs

It is estimated that 91% of businesses in South Africa are small, medium and micro size enterprises (SMMEs) and they account for between 52% and 57% of South Africa's gross domestic product (Abor & Quartey, 2010). This comprises a large portion of the South African economy and therefore these businesses should be protected appropriately to ensure their sustainability.

As can be seen in the Table 1, micro-sized enterprises have from 1 to 5 employees, small-sized enterprises have from 6 to 50 employees and medium-sized enterprises have from 51 to 200 employees. **Enterprises with more than 200 employees will be regarded as large enterprises and will not be included in the scope of this study**.

Table 1: Enterprise classifications used in this dissertation.

| Size of Class | The total full-time employees |
|---|---|
| **Micro enterprises** | 1-5 employees |
| **Small enterprises** | 6-50 |
| **Medium enterprises** | 51-200 |
| **Large enterprises** | More than 200 |

In the past, WLANs have been seen as a slow and unreliable network standard (Chen, Katsaros, Nanopoulos, & Manolopoulos, 2005). The 802.11g standard, which was ratified in 2003, is now seen as inadequate because applications have become more complex and require more bandwidth. The 802.11g standard struggled to do streaming of video data efficiently because of the speeds that it offered.

The new 802.11ac standard, which was ratified in 2012, uses newer technologies and tweaks the existing technologies to give WLANs more speed and range. The speed obtainable when using 802.11ac is up to 1300Mbps making WLANs a sustainable choice for SMMEs (Eldad & Stacey, 2013).

The benefits of using WLANs in SMMEs are the following (Chandra, et al., 2009):

- Mobility - WLAN users have the ability to access shared resources without looking for a place to plug in, anywhere in the organisation. A WLAN allows users to be truly mobile as long as the WLAN device is within the network coverage area.
- Range of coverage - The range of a typical WLAN access point is about 100 metres. WLAN access points can extend the cover of an area in such a way that the range of coverage overlaps each other providing roaming. Thereby the WLAN user can wander around and move from the coverage area of one access point to another while maintaining seamless connection within the network.
- Ease of use – WLANs are easy to use and the users need minimum experience to take advantage of them.
- Flexibility – The installation of a WLAN infrastructure can be fast and easy and can eliminate the need to pull cable through walls and ceilings. WLANs can be set up where wires may be impossible to install.
- Scalability – WLANs can be designed to be extremely simple or complex. They can support large numbers of WLAN devices and large physical areas by adding access points to extend coverage.
- Cost – The cost of installing and maintaining a WLAN is on average lower than the cost of installing and maintaining a traditional wired LAN. This is because WLANs eliminate the direct costs of cabling and the labour associated with installing and repairing it. WLANs also are simple to move and change which reduces the ongoing administrative costs.

When comparing the benefits that WLANs bring to an SMME against the total cost of ownership (TCO) it can be seen that using WLANs can bring more value to a business, provided that the WLAN is secured and managed properly (Cisco Systems, Inc, 2003).

The securing and management of WLANs is therefore important and requires much attention especially in view of the fact that WLANs tend to be exposed to more threats than wired networks.

SMMEs in particular do not usually have on-site security support personnel and may not have funds to outsource WLAN security functions. This implies the lack of the required knowledge, skills and resources in SMMEs pertaining to securing WLANs.

It will therefore be more useful for SMMEs to have access to guidelines which may be derived from accepted international information security control frameworks and standards and then be used for their own in-house implementation and securing of WLANs.

## 3.3 Information Security Control Frameworks

When implementing something in the correct manner and ensuring effectiveness, it is useful to have a benchmark that has been developed using international best practices. With regards to information security there are many security control framework standards which are recognised internationally as providing useful guidelines for adequate implementation of information security in organisations. By using a recognised information security framework one can ensure confidentiality, integrity and availability of all information technology (IT) assets within an organisation.

A control framework is a "structured way of categorising controls to ensure the whole spectrum of a control is covered adequately" (ISACA, 2012). A number of information security control frameworks have already been listed further above in this paper.

The information security control frameworks listed all have implications on the objectives of this research study. However, due to the magnitude of the research involved in analysing each framework only three were selected. The control frameworks selected are COBIT 5 for Information Security, ISO/IEC 27002 and ISF Standard of Good Practice. The COBIT 5 framework was selected because it is the only framework for governance and management of business and IT. The ISO/IEC 27002 was selected because it gives detailed guidelines for information security practices and it is widely used amongst organisations. The ISF Standard of Good Practice was selected because the body that created it is seen as the world's leading authority on information security and the ISF is made up of thousands of information security specialists worldwide.

Going through these information security control framework standards it can clearly be seen that they are aimed at larger organisations. For example, COBIT 5 BAI05 requires a qualified information security professional to serve on all IT implementation teams. ISO 27002 A.6 Organization Information Security states that information security activities should be co-ordinated by representatives with relevant expert roles and job functions. ISO 27002 A.15 Compliance indicates that a specific data protection officer should provide guidance to managers on the responsibilities and specific procedures that should be followed. ISF SoGP SG1.1 requires that a full time Chief Information Security Officer be appointed in the organisation. In ISF SoGP SR2.1, it requires the establishment of a high-level working group to manage information privacy issues.

While these specialized information security personnel may be found in larger organisations, small organisations would not typically have an employee dedicated to these tasks.

The information security control frameworks researched in this study were therefore not specifically created with small, medium, and micro enterprises (SMMEs) in mind. The frameworks are exhaustive and therefore not suitable for SMMEs. They were aimed at larger corporations and are not freely available, requiring extensive resources to purchase. The controls in the frameworks are typically aimed at experienced security professionals such as Information Security Officers. They are too complex for ordinary SMME staff to understand and implement. Adding to this, the control frameworks are not specifically related to securing WLANs although there may be a few controls that can be made applicable.

# 4. A WLAN SECURITY CONTROL FRAMEWORK FOR SMMES

In this section the WLAN Security Control Framework for SMMEs is presented. The framework consists of a control matrix table and detailed control tables for physical, technical and operational security. However, for the sake of brevity, detailed control tables were removed and only the control matrix table is presented here and appended with reference to the information security control frameworks which were used as sources of information.

In order to explain how the WLAN Security Control Framework was developed, a walkthrough will be demonstrated below.

1. Take the example of “APO07: Manage Human Resources” from COBIT.
2. A control activity for securing WLANs in SMMEs was created having looked at APO07. This control activity was defined as “Train staff on the general risks of WLANs”.
3. A control objective was derived “To provide staff with the skills required to protect against the general risks of WLANs” and a detailed description was provided for the control activity.
4. Decision was made as to which general security area this falls under, namely, physical security, technical security, or operational security.
5. A reference code was added to the control activity name, in this case “PS04” as it falls under physical security (PS).
6. A relevance indication was added i.e. Fundamental (F) if it is applicable to all organisations or Specialised (S) if it is applicable to only specific organisations. PS04 is of fundamental relevance.
7. SMME classification was provided to indicate whether this is applicable to micro, small and/or medium enterprises. PS04 is applicable to small and medium enterprises.
8. The threats that may be possibly mitigated by this control activity were indicated. In this case, PS04 can mitigate social engineering, physical, and environmental threats.
9. Finally, all the original information security control framework references were provided to allow the reader to investigate more detail regarding the control activity. In this case, APO07 from COBIT 5 is similar to A.8 and A.9 from ISO 27002, and CF2 from ISF SoGP.
10. These steps were repeated for all the COBIT 5 domains, ISO 27002 clauses, and ISF SoGP categories deemed applicable to securing WLANs in SMMEs.

All of the information described above can be found in a summary control matrix for the WLAN Security Control Framework. Further detailed information for the thirty-six control activities were also created and they list the Physical Security (PS), Technical Security (TS), and Operational Security (OS) detail for the framework respectively.

*Note: The order of the security areas in this WLAN Security Control Framework does not imply their importance. All security areas are important therefore each organisation should apply the control activities that are applicable to their size.*

In Figure 1, the links are depicted between the information security control frameworks and the three security areas. All the control frameworks had components that were relevant to all the security areas used in the WLAN Security Control Framework. The framework is shown in Table 2.

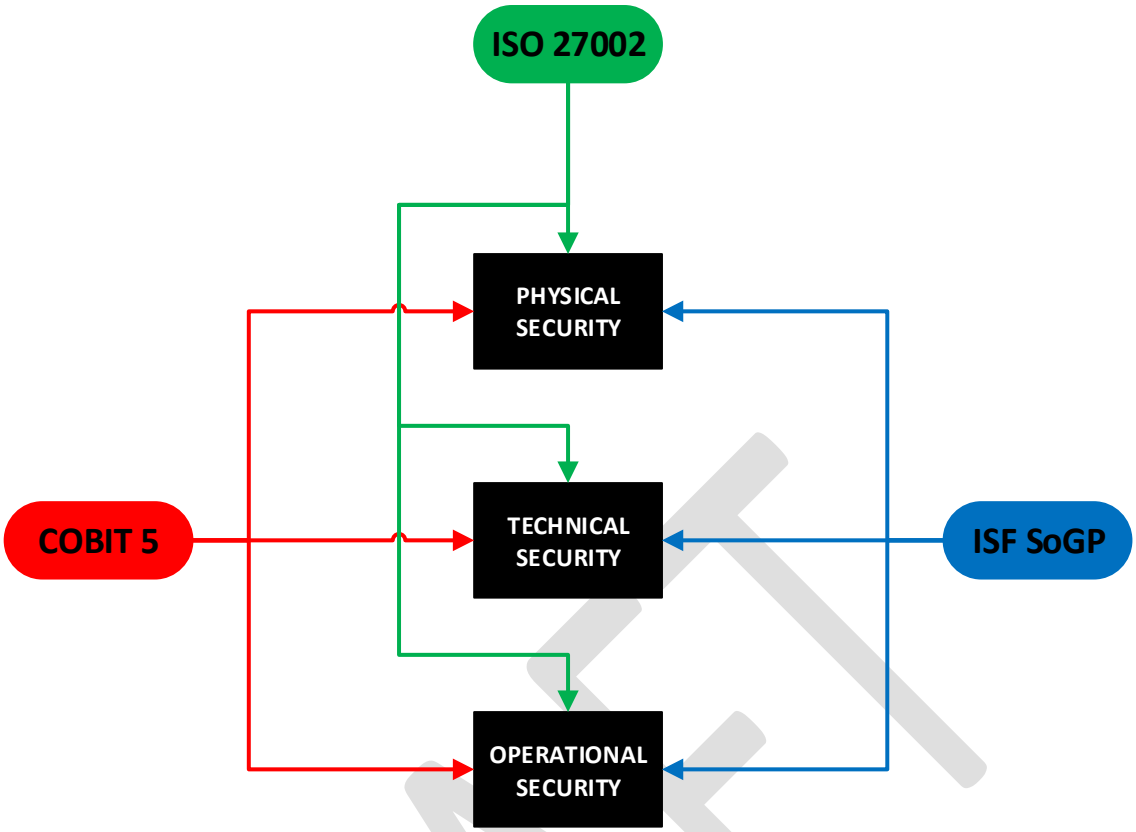



Figure 1: From Information Security Control Frameworks to Security Areas adopted in the WLAN Security Control Framework

Table 2: WLAN Security Control Framework Matrix.

| REFERENCE | CONTROL ACTIVITY | RELEVANCE | MICRO | SMALL | MEDIUM | INFORMATION SECURITY CONTROL FRAMEWORKS REFERENCES | THREATS MITIGATED | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | MALWARE | HACKING | SOCIAL ENGINEERING | MISUSE | PHYSICAL | ERROR | ENVIRONMENTAL |
| **PS01** | **Secure antennas and related cabling supporting WLANs.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.9**<br>**ISF SoGP: CF9, CF19** | | ✓ | | | ✓ | | ✓ |
| **PS02** | **Secure WLAN access points.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.9**<br>**ISF SoGP: CF9, CF19** | | | | | ✓ | | ✓ |
| **PS03** | **Secure WLAN client devices.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.7, A.9, A.11**<br>**ISF SoGP: CF14, CF19** | | | | | ✓ | | ✓ |
| **PS04** | **Train staff on the general risks of WLANs.** | F | | ✓ | ✓ | **COBIT 5: APO07**<br>**ISO 27002: A.8, A.9**<br>**ISF SoGP: CF2** | | | ✓ | | ✓ | | ✓ |
| **PS05** | **Control access to secure areas.** | S | | | ✓ | **COBIT 5: DSS05, MEA02**<br>**ISO 27002: A.9, A.11**<br>**ISF SoGP: CF19** | | | ✓ | | ✓ | | ✓ |
| **PS06** | **Conduct regular WLAN site surveys.** | S | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF9** | | ✓ | ✓ | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PS07** | **Secure antennas as to minimise coverage.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF9** | | ✓ | | | | | |
| **PS08** | **Deploy redundant WLAN access points.** | F | | ✓ | ✓ | **COBIT 5: BAI04**<br>**ISO 27002: A.14**<br>**ISF SoGP: CF9, CF20** | | | | | ✓ | | ✓ |
| **PS09** | **Secure backups.** | F | | | ✓ | **COBIT 5: DSS04**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF7** | | | | ✓ | ✓ | ✓ | ✓ |
| **PS10** | **Protect WLAN access points with UPS.** | F | | | ✓ | **COBIT 5: DSS01**<br>**ISO 27002: A.9**<br>**ISF SoGP: CF19** | | | | | | ✓ | ✓ |
| | | | | | | | | | | | | | |
| **TS01** | **Secure the SSID.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10**<br>**ISF SoGP: CF7, CF9** | | ✓ | | ✓ | | | |
| **TS02** | **Configure authentication.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10, A.11**<br>**ISF SoGP: CF6, CF8, CF9** | | ✓ | | | | | |
| **TS03** | **Configure MAC address filtering.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10, A.11**<br>**ISF SoGP: CF9** | | ✓ | | | | | |
| **TS04** | **Secure default WLAN access point settings.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6, CF7** | | ✓ | | | | | |
| **TS05** | **Require a valid password prior to administrator access.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6, CF14** | | ✓ | | ✓ | | ✓ | |
| **TS06** | **Configure user accounts.** | F | | ✓ | ✓ | **COBIT 5: DSS05, DSS06**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6** | | ✓ | | ✓ | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **TS07** | **Disable unused and dormant user accounts.** | F | | ✓ | ✓ | **COBIT 5: APO07, DSS05**<br>**ISO 27002: A.8, A.11**<br>**ISF SoGP: CF2, CF6** | | | ✓ | | ✓ | | | |
| **TS08** | **Configure strong passwords.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6, CF8** | | | ✓ | | ✓ | | | |
| **TS09** | **Disable responses to broadcast SSID probe.** | S | | | ✓ | **ISF SoGP: CF9** | | | ✓ | | | | | |
| **TS10** | **Perform user identification.** | F | | ✓ | ✓ | **COBIT 5: DSS06**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF6, CF8** | | | ✓ | | ✓ | | | |
| **TS11** | **Segregate WLANs from internal network.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF7, CF9** | | ✓ | ✓ | | | | | |
| **TS12** | **Secure gateways prior to accessing the internal network.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10, A.11**<br>**ISF SoGP: CF6, CF9** | | ✓ | ✓ | | | | | |
| **TS13** | **Secure management interface on WLAN access points.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10, A.11**<br>**ISF SoGP: CF7, CF9** | | | ✓ | | ✓ | | | |
| **TS14** | **Secure SNMP.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.11**<br>**ISF SoGP: CF9** | | | ✓ | | ✓ | | | |
| **TS15** | **Enable WPA2 encryption.** | F | ✓ | ✓ | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10, A.11**<br>**ISF SoGP: CF9** | | | ✓ | | | | | |
| **TS16** | **Encrypt WLAN devices.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.9**<br>**ISF SoGP: CF14** | | | ✓ | | | ✓ | | |
| **TS17** | **Encrypt data using high level protocols.** | F | | | ✓ | **COBIT 5: DSS05**<br>**ISO 27002: A.10** | | | ✓ | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | ISF SoGP: CF9 | | | | | | | | |
| **TS18** | **Update WLAN device firmware.** | F | ✓ | ✓ | ✓ | COBIT 5: DSS05<br>ISO 27002: A.12<br>ISF SoGP: CF10 | | ✓ | ✓ | | | | | |
| | | | | | | | | | | | | | | |
| **OS01** | **Direct and monitor the WLAN Security Control Framework.** | F | | ✓ | ✓ | COBIT 5: EDM01, APO13<br>ISO 27002: A.5<br>ISF SoGP: SG1 | | | | | ✓ | | | |
| **OS02** | **Document a WLAN Security Policy.** | F | ✓ | ✓ | ✓ | COBIT 5: APO01<br>ISO 27002: A.5<br>ISF SoGP: CF1 | | | | | ✓ | | | |
| **OS03** | **Distribute WPA2 encryption keys when changed.** | F | ✓ | ✓ | ✓ | COBIT 5: DSS06<br>ISO 27002: A.10<br>ISF SoGP: CF7, CF9 | | | | | | | ✓ | |
| **OS04** | **Audit WLAN access points.** | F | | ✓ | ✓ | COBIT 5: MEA02<br>ISO 27002: A.10, A.15<br>ISF SoGP: SI1 | | | ✓ | | ✓ | | | |
| **OS05** | **Review log files.** | F | | ✓ | ✓ | COBIT 5: MEA02<br>ISO 27002: A.10<br>ISF SoGP: SI1, CF10 | | | ✓ | | ✓ | | ✓ | |
| **OS06** | **Store WLAN access point firmware versions.** | F | | | ✓ | COBIT 5: BAI10<br>ISO 27002: A.10<br>ISF SoGP: CF9, CF14 | | | | | | | ✓ | |
| **OS07** | **Store WLAN information.** | F | | | ✓ | COBIT 5: BAI10<br>ISO 27002: A.10<br>ISF SoGP: CF6, CF9 | | | | | | | ✓ | |
| **OS08** | **Establish a data backup and recovery plan.** | F | | | ✓ | COBIT 5: DSS04<br>ISO 27002: A.14<br>ISF SoGP: CF7, CF20 | | | | | ✓ | | ✓ | ✓ |

# 5. CONCLUSION

This paper presented the WLAN Security Control Framework for SMMEs.

The WLAN Security Control Framework was developed from a number of international standards, namely, COBIT 5 for Information Security (COBIT 5), ISO/IEC 27002:2005 (ISO 27002) and the ISF Standard of Good Practice 2012 (ISF SoGP). The contents of the framework were separated into three security areas, namely, Physical Security, Technical Security, and Operational Security. Each item in the framework presented controls that assist in mitigating identified threats to SMMEs in South Africa.

The validation of the framework was done using a focus group. The main aim of the focus group was to ascertain whether this research study has contributed in addressing the gaps identified in current approaches for securing WLANs in small, medium, and micro enterprises (SMMEs).

At the end of this validation it was concluded that the WLAN Security Control Framework was logically set out, easy to use, recommended sensible and appropriate controls for the given scenarios and was thus deemed to have served its purpose. The researcher does however take cognisance of the fact that certain small businesses might require training in the use of the framework.

The results from the focus group therefore agreed that this research study contributed in addressing the identified gaps in current approaches for securing WLANs in SMMEs. Thus, it can be concluded that the developed WLAN Security Control Framework was deemed valid.