AN INVESTIGATION OF ISO/IEC 27001 ADOPTION IN SOUTH AFRICA

Submitted in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

At

RHODES UNIVERSITY

By

CHRISTO COETZER

JANUARY 2015

Abstract

The research objective of this study is to investigate the low adoption of the ISO/IEC 27001 standard in South African organisations. This study does not differentiate between the ISO/IEC 27001:2005 and ISO/IEC 27001:2013 versions, as the focus is on adoption of the ISO/IEC 27001 standard.

A survey-based research design was selected as the data collection method. The research instruments used in this study include a web-based questionnaire and in-person interviews with the participants.

Based on the findings of this research, the organisations that participated in this study have an understanding of the ISO/IEC 27001 standard; however, fewer than a quarter of these have fully adopted the ISO/IEC 27001 standard. Furthermore, the main business objectives for organisations that have adopted the ISO/IEC 27001 standard were to ensure legal and regulatory compliance, and to fulfil client requirements.

An Information Security Management System management guide based on the ISO/IEC 27001 Plan-Do-Check-Act model is developed to help organisations interested in the standard move towards ISO/IEC 27001 compliance.

Keywords: ISO/IEC 27001; ISMS; information security; risk management; information security framework

Declaration

I, Christo Coetzer, hereby declare that

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

C.COETZER

ACM Computing Classification System Classification

Thesis classification under the ACM Computing Classification System[1] (2012 version, valid through 2014):

General and reference: Document types

Security and privacy: Formal methods and theory of security

Security and privacy: Human and societal aspects of security and privacy

[1] http://www.acm.org/about/class/2012/

Acknowledgement

I would like to thank my supervisor, Dr Karen Bradshaw, who assisted me in the completion of this dissertation. Her knowledge, guidance, and support played a major role throughout this exercise. I also would like to thank the participants who committed time to participate in the research survey.

I especially want to thank my wife, and family members for their support and patience while I was busy with the completion of this dissertation. Without their support, I would not have been able to complete this task.

Table of Contents

List of Tables

List of Figures

Glossary

The following definitions of terms and abbreviations are used in this dissertation, and are related to the terms and definitions of the ISO/IEC 27001 standard (ISO/IEC 27001 2005):

Accreditation - *Process by which an authorized organisation officially recognizes the authority of a certification body to evaluate, certify and register an organisation's ISMS with regard to published standards.*

Adopt - *Implementation of the ISO/IEC 27001 standard and registered for certification*

Align – *Implementation of only portions of the ISO/IEC 27001 standard for internal organisational use*

Asset – *Any tangible or intangible object that has value to the organisation*

Availability – *To be accessible and usable upon demand*

BS - *British Standard*

BSI - *British Standards Institute*

Certification – *The authoritative act of documenting compliance with agreed requirements*

COBIT - *Control Objectives for Information and related Technology*

Compliance - *An assessment to verify whether a system that has been implemented complies with a standard*

Confidential – *Only accessible to authorised entities*

Control - *A means of managing risk in the form of policies, procedures, or guidelines*

Information – *Meaningful data*

Information security – *Preservation of information confidentiality, integrity and availability according to the information security triad*

Information Security Management System – *Portion of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security*

IT – *Information technology*

ITIL – *Information Technology Infrastructure Library*

Integrity – S*afeguarding the accuracy and completeness of information*

ISO/IEC - *International Organisation for Standardisation / International Electrotechnical Commission*

ISMS – *Information Security Management System*

JTC - *Joint Technical Committee*

Large organisation - *Organisation with more than 2000 employees*

Medium organisation - *Organisation with 50 to 200 employees*

Medium-to-large organisation - *Organisation with 200 to 2000 employees*

Organisation – *A group of people and facilities with an arrangement of responsibilities, authorities and relationships*

PDCA - *Plan-Do-Check-Act*

Registration – *Certification has been recorded, or registered, with the auditing body*

Risk analysis – *Systematic use of information to identify sources and to estimate the risk*

Risk evaluation – *Process of comparing the estimated risk against given risk criteria to determine the impact and severity of risk*

Risk assessment – *Process of risk analysis and risk evaluation*

Risk treatment – *Treatment process of selection and implementation of controls to manage risk activities*

Risk management – *Management of risk activities*

SABS - *South African Bureau of Standards*

SANS - *South African National Standards*

Small organisation: *Organisation with fewer than 50 employees*

Statement of Applicability (SOA) - *Document describing the control objectives and controls that are relevant and applicable to an ISMS, based on the results and conclusions of the information security risk assessment and risk treatment processes*

TAM - *Technology acceptance model*

Threat – *Cause an unwanted security incident that will cause damage to a system*

Vulnerability – *Weakness of an asset that can be exploited by a threat*

Chapter 1: Introduction

In the past several years, information security has become an important aspect of South African organisations. Organisations are slowly starting to realise that the installation of yet another security hardware appliance such as a firewall, is not sufficient to enhance the security posture of their organisation. The latest security technology will not provide the security that organisations expect if the people and processes that form part of it are not in place or adhered to. Internet usage globally, from first world to developing countries, is constantly rising with the usage of the Internet ranging from businesses to individuals sharing information (InternetWorldStats 2012). According to the Verizon Data Breach Investigation Report, more than 47000 security incidents have been reported between 2012 and 2013 (Verizon 2013). From an information security perspective, this has created severe concerns regarding the security of information. Organisations and individuals need to realise the importance of information security and take the relevant steps to ensure the protection thereof.

There are various best practice frameworks available for organisations to assess security risks, and implement controls to comply with government regulations. The International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) published a set of standards (ISO) that organisations can use to improve their security posture by using these standards as the basis of a security framework. These standards provide guidance to organisations to create a secure Information Security Management System (ISMS). Organisations have the choice to implement an ISMS as an approach to secure and manage confidential information as it encompasses people, processes and technology.

Previous research in the field of information security management has identified the factors influencing information security management as well as the interpretation and the application of available approaches to information security management (Eloff & von Solms 2000; Yildirim et al. 2011). Research has also suggested that the protection of sensitive organisational information should be driven from the board of an organisation and should form part of corporate governance (Posthumus & von Solms 2004). No specific research to the adoption of the ISO/IEC 27001 standard by South African organisations has been performed.

During the engagement with several organisations regarding this research, a general understanding and insight of the perception that organisations have of an ISMS, especially towards the ISMS described in the ISO/IEC 27001 standard, was obtained. To adopt ISO/IEC 27001 there has to be an understanding of the standard, as well as a business objective. The combination of a business objective and information security to adopt ISO/IEC 27001 is the theme of this research.

1.1 Context of the Study

The protection of information, whether for business or personal reasons, is a critical requirement that needs to be addressed in today's era. To assist in enforcing this, governments legislate corporate governance that organisations are required to adhere to, and which provides a level of surety that sensitive information is being secured to a certain degree (IoDSA 2009). International standards, frameworks and models have been developed to assist organisations to ensure the protection of information, with the ISO/IEC 27001 standard being one of them (ISO/IEC 27001 2013).

Organisations can align to ISO/IEC 27001 merely to implement it and meet basic security requirements, or at the end of an implementation they can pursue registration with the aim of receiving a certificate that shows adherence to and adoption of the standard. The certificate provides evidence that the organisation in question is able to manage the protection of sensitive information assets, and can be used to provide assurance of this to any third party including clients. The adoption of the standard provides organisations with the ability to identify and mitigate information security risks (ISO/IEC 27001 2013). This approach will enhance the overall information security posture and provide confidence to relevant parties that the organisation is capable of managing information security using a risk based approach.

International organisations that are seeking to adopt and obtain successful registration of the standard, are doing so with the objective that the registration will provide the surety that the security measures and controls implemented, meet international information security requirements (Saint-Germain 2005). Such international requirements include Australia's Privacy Act (PA 1988); France's Data Protection Act (DPA 1978); Germany's Federal Data Protection Act (FDPA 2001); and the United Kingdom's UK Data Protection Act (DPA 1998).

Globally, organisations still have a very low uptake of adopting an information security framework, although this has slowly increased over the past few years (ISACA 2011). As per the ISO 2012 survey that focussed on the global distribution of ISO/IEC 27001, it is clear that there is a healthy growth in the adoption of the ISO/IEC 27001 standard, as it has spread from 64 countries in 2006 to 103 countries in 2012 (ISO 2012). Globally Japan holds the most certificates, with the United Kingdom in second place. In Africa, South Africa and Egypt are the top holders of certificates. The results of the survey also show the evolution of the adoption of ISO/IEC 27001 in South Africa as it has grown from five organisations in 2006 to 22 in 2012.

South African organisations choosing to adopt ISO/IEC 27001 may have different motives and business objectives for doing so. The aim of this research is to investigate the adoption of ISO/IEC 27001 within South African organisations.

1.2 Problem Statement

This research aims to investigate the knowledge and understanding of the ISO/IEC 27001 standard within South African organisations. It also investigates who has adopted the ISO/IEC 27001 standard across various sized organisations and industries. Further, we investigate the business objective(s) in adopting ISO/IEC 27001, as well as identifying the benefits gained and challenges the organisations faced with the adoption of the ISO/IEC 27001 standard.

The problem addressed in this study is the low adoption rate of the ISO/IEC 27001 standard in South African organisations.

The research question posed is the following:

Why have so few organisations adopted the ISO/IEC 27001 standard in South Africa?**.**

Research Objectives

To answer the research question posed above, we set the following objectives:

- To determine what knowledge South African organisations have of the ISO/IEC 27001 standard;
- To determine who has adopted the ISO/IEC 27001 standard in South Africa;

- To determine the business objective(s) in adopting the ISO/IEC 27001 standard;
- To evaluate the benefits and challenges organisations face with the adoption of the ISO/IEC 27001 standard.

1.3 Methodology

To investigate the adoption of ISO/IEC 27001 in South Africa, a web-based questionnaire as well as several semi-structured in-person interviews were conducted to understand current practice. The questionnaire and interviews focussed on various South African organisation industries and sizes to determine the knowledge South African organisations have of ISO/IEC 27001, who is adopting ISO/IEC 27001, the business objectives underlining the adoption of ISO/IEC 27001, as well as the benefits, and challenges in adopting ISO/IEC 27001. Results obtained lead to a reasonable conclusion of the nature of the adoption of ISO/IEC 27001 within organisations.

1.4 Limitations of the Study

- This study does not differentiate between the ISO/IEC 27001:2005 and ISO/IEC 27001:2013 versions, as the focus is on the adoption of the ISO/IEC 27001 standard per se.
- References for this study mostly refer to the ISO/IEC 27001:2005 version as ISO/IEC 27001:2013 was only recently released, with limited adoption thus far.
- This study does not deal with the adoption of any other industry best practice, framework or standard in South African organisations.
- This study does not focus on the in-depth investigation of the ISO/IEC 27002 code of practise for information security controls used in the audit process of an ISO 27001 ISMS, but rather on the adoption of the ISO/IEC 27001 standard.
- Due to the sensitive nature of organisations disclosing information regarding their adoption of the standard, the sample size is small.

1.5 Assumptions

This dissertation is an investigation of the adoption of ISO/IEC 27001 by South African organisations. The research includes the investigation of several organisations of varying size and industry to determine the reasons for adopting the standard. The validity of the results depends on the following assumptions:

- The organisations have the relevant knowledge of the ISO/IEC 27001 standard when deciding whether to adopt the standard.
- The adoption of the standard is most feasible in medium and large sized companies. This assumption can be made as the implementation of the standard is a timely exercise, and auditing is expensive. These factors could therefore reduce the cost-to-benefit ratio for smaller organisations.

1.6 Significance

The requirement for organisations to protect confidential information is on the rise, and the South African Protection of Personal Information Act (POPI) (POPI 2013) is a clear indication thereof. Failure to protect confidential information will result in various damages to the organisation. Security standards such as ISO/IEC 27001 provide organisations with a structured approach to manage and secure confidential information. This research determines why organisations adopt ISO/IEC 27001.

Although this study was conducted with a relatively small sample, the objective was to find preliminary results. This study provides a starting point to ascertain the status of ISMSs specifically towards the ISO/IEC 27001 standard within a South African context. Based on these results, further research can be conducted.

Furthermore, an ISMS management guide based on the ISO/IEC 27001 Plan-Do-Check-Act (PDCA) model has been developed to help organisations interested in the standard, move towards ISO/IEC 27001 compliance.

1.7 Summary

The dissertation consists of the following chapters:

- **Chapters 2 and 3**: Literature Review: This review covers background concepts of various forms of governance and information security in general, as well as details of the ISO/IEC 27001 standard focussing on the key elements for an ISMS.
- **Chapter 4**: Methodology: This discusses the approach followed with justifications to collect the required data for the research.
- **Chapter 5**: Survey Findings and Analysis: Findings and analysis of the collected data for investigation of ISO/IEC 27001 adoption in South Africa are presented in this chapter.

- **Chapter 6**: Discussion of Survey Results: The discussion of the results of the survey findings and analysis are presented in this chapter.
- **Chapter 7**: Conclusion and Future Work: This chapter summarises the completed research and highlights the findings thereof. It also discusses possible future work.

Chapter 2: Background Concepts

In this chapter, we discuss the relationship between corporate, information technology (IT) and information security governance, and provide an overview of information security risk management, information security management, information security compliance and frameworks.

2.1 Corporate Governance

Before we delve into information security frameworks, we need to understand the main drivers thereof. Organisations need to adhere to governance practice; this includes corporate governance, IT governance and information security governance. Adopting these practices ensure that the organisation's business and IT management support, maintain and extend the organisation's strategies and objectives (ITGI). Corporate governance has to do with an organisation's senior management's accountability towards its stakeholders for the use of organisational assets and to act in the stakeholder's interest (Poore 2006). As per Poore (2006), the corporate structure distributes rights between the following standard groups:

- The shareholders and owners of an organisation;
- The board of directors of an organisation;
- The managerial level;
- The employee / worker level.

The structure of corporate governance consists of several aspects, namely national and international laws that govern the establishment of corporate bodies, the organisational structure of the corporate body as well as any bylaws designed by the corporate body (Poore 2006).

The objective of corporate governance is to provide the rules and procedures for any decisions made regarding corporate affairs (IoDSA 2009). Corporate governance also consists of the structure that is required to set the corporate objectives; this includes the means of achieving as well as monitoring performance against the set of objectives. Two well-known corporate governance committees are the Committee of Sponsoring

Organisations[2] (COSO) and local to Southern Africa, the Institute of Directors in Southern Africa[3] (IoDSA).

The COSO of the Treadway Commission created and published a governance document in 1985 called "Internal Control – Integrated Framework" (Moeller 2007), which provides a control-based foundation for corporate governance. COSO deals with the three related subjects: enterprise risk management, internal control, and fraud deterrence.

The IoDSA with the assistance of retired Supreme Court of South Africa Judge Mervyn E. King commissioned the King Committee in 1992 to develop a set of principles to promote the standards of corporate governance within organisations in South Africa (IoDSA 2009). The released report from the committee was called the King Report and was progressively updated and published in 1994 (King I), 2002 (King II), and 2009 (King III). The release of King III required that all publicly listed companies were expected to comply with the code. From an IT governance perspective, one of the main changes made in the latest King III report was the inclusion of IT governance (IoDSA 2009). The King III report is the only report of the three currently available from the IoDSA.

The Saytam (Forbes 2009), Bernie Madoff (Forbes 2008) and Lehman Brothers (Investopedia 2009) scandals are just some of the examples of failed corporate governance. Because of such incidents, new legislation such as the Sarbanes-Oxley Act of 2002 (SOX 2002), and the South African Companies Act of 2008 (CA 2008) have raised the level of importance of corporate governance.

The results of the research paper by Nitm (2013) investigating the relationship between an integrated corporate governance index and financial performance, showed that investors reward organisations with better corporate governance with higher financial incentives. Good corporate governance practices are important as these reduce corporate failures and can assist organisations to attract investments (local and abroad). The efforts made by institutes such as the IoDSA and the King Committee to improve corporate governance standards and practices in South African companies are commendable.

[2] www.coso.org
[3] www.iodsa.co.za

2.2 Information Technology Governance

With the growth in IT, the need for IT governance has become a critical facet within the context of corporate governance. The effective and efficient management and governance of IT ensures that IT supported business objectives optimise the investment in IT as well as manage IT risks in the business (Poore 2006). In 1988, the Information Systems Audit and Control Association[4] (ISACA) formed a non-profit independent research entity called the Information Technology Governance Institute[5] (ITGI). The objective of the ITGI was to identify and develop governance principles that supported IT within organisations (ITGI). In 2010 the ITGI commissioned Price Waterhouse Coopers in Belgium to conduct a global market research on the governance of enterprise IT (ISACA 2011). One of the key findings of this report was that the governance of enterprise IT was a priority with most of the organisations, and the main driver thereof was the assurance that IT aligns with the business objective(s).

The 1992 Cadbury Report (Cadbury 1992), and the 1999 Turnbull Report (Turnbull 1999) were two of the early reports that played a role in influencing the maturity of IT governance. The Financial Reporting Council (FRC), the London Stock Exchange, and the accountancy profession on the Financial Aspects of Corporate Governance established the Cadbury Committee in 1991 and released the Cadbury Report in 1992, which reported on the financial aspects of corporate governance. In 1999, the Turnbull report was published by the FRC and was used to set out the best practices on internal control for United Kingdom listed organisations.

According to Poore (2006), IT governance is concerned with the following:

- to deliver value to the organisation;
- to mitigate IT risks to the organisation.

A number of frameworks and standards are available to develop and implement an IT governance structure within an organisation, but these require collaboration and teamwork between business management and IT. These two management groups, one focused on business and strategic concepts, and the other on technological concepts, are required to have the same understanding of the deliverables from the control frameworks when implementing

[4] www.isaca.org
[5] www.itgi.org

IT governance principles. Different understandings and implementations of such frameworks and standards have created misalignment between IT principles and business objectives and ultimately an ineffective IT governance system (Goosen & Rudman 2013). To avoid this, an integrated framework or standard is required to ensure an effective implementation of IT governance within an organisation.

Frameworks such as King III (IoDSA 2009), ISO/IEC 38500:2008 (ISO/IEC 38500 2008), Control Objectives for Information and related Technology (COBIT) (COBIT 2012), and Val IT (VALIT 2008), together with some more detailed standards such as Information Technology Infrastructure Library (ITIL) for IT service delivery (ITIL 2011) and the Capability Maturity Model Integration for solution delivery (Kneuper 2008) have been developed to provide the context in which to embed IT governance at organisations.

The release of the third King Report on Corporate Governance (King III) in 2009 highlighted the requirements and implementation of more effective IT governance principles owing to the changing nature of IT environments in organisations (IoDSA 2009). King III required that business management and IT work together to implement these principles. This should not be seen as a pure IT responsibility as the report clearly states that directors and senior managers should ultimately be held responsible for the implementation of good IT governance principles within an organisation (IoDSA 2009). The King III report includes a section on information security, where the board of an organisation is required to ensure that information is adequately protected and that an ISMS is developed and implemented (IoDSA 2009).

The release of the international standard ISO/IEC 38500: 2008 titled "*Corporate governance of information technology*" (ISO/IEC 38500 2008), is a mark that shows the importance of IT governance and its applicability to organisations across the globe. ISO/IEC 38500:2008 assists organisations to clarify IT governance using a top-down approach by describing senior management's accountability towards their stakeholders in the use of IT resources and activities by ensuring that the appropriate IT governance and information security frameworks exist by covering the following (ISO/IEC 38500 2008):

- Responsibility
- Strategy
- Acquisition (and implementation)

- Performance
- Conformance
- Human behaviour

The benefit of the ISO/IEC 38500:2008 IT governance framework is to ensure that accountability is assigned for all IT related risks and activities throughout the organisation (ISO/IEC 38500 2008). This includes assigning and monitoring IT security accountability, responsibility, strategies and behaviours so that measures and controls are established and implemented for reporting on and responding to the use of IT in the organisation.

The ITGI developed COBIT and the Val IT Framework for Business Technology Management (ITGI). COBIT is an internationally accepted framework for the implementation of IT governance. The good practises in the COBIT framework are a common approach to effective and efficient IT control. COBIT supports the principles mentioned in the ISO/IEC 38500 standard as well as those in the King III Code (COBIT 2012). ISACA's Val IT Framework for Business Technology Management addresses IT governance by assessing and addressing various tasks such as risk and costs related to an organisation's portfolio of IT-enabled business investments (VALIT 2008). Organisations can adapt the use of frameworks and standards to cater for their requirements. By aligning standards such as COBIT and ISO/IEC 27001 that provide organisations with guidance on "*what*" should be done, with ITIL that provides the "*how*" regarding service managament, management of quality and reliability in organisations can be enhanced, which assists in adherence to relevant regulatory and contractural requirements as well (ISACA 2008).

Although the two are not congruent, IT governance is an important aspect of information security governance. IT governance addresses the value that technology provides to an organisation. Often the selection of technology to deliver the value to the organisation is in opposition to the effectiveness of information security. An example of this is the deployment of an off-the-shelf wireless network solution for the use of web based applications and local network access. Such a solution would permit IT to deliver a valued solution to the organisation, but the solution would not cater for the pillars of information security consisting of confidentiality, integrity and availability of the organisation's information, that would be available on that network. Such a solution may conflict with IT governance in the sense that

the mitigation of IT risks are not met, but this is where information security governance should be able to guide the organisation to a more secure solution.

2.3 Information Security Governance

Information has become a valuable asset for organisations. Information assets can range from an organisation's employees to the raw data. Human resource departments state that employees are the most important asset of an organisation, even though organisations intentionally downsize such assets when required to stay in business. Information assets provide a source of competitive advantage as well as being used to generate capital for organisations. An information asset can also become a liability to the organisation as it could lead to a negative value that surpasses the investment the organisation had in it.

As discussed in the corporate governance section of this chapter, it is clear that the main purpose of governance is for senior management to be held accountable to the stakeholders of the organisation. Posthumus and von Solms (2004) motivate that there is a requirement to incorporate information security in corporate governance. This could be achieved by developing an information security governance framework. The purpose of information security governance is to hold senior management accountable for the protection and safeguarding of information assets within the organisation. Information security governance should be an essential part of corporate governance, and aligned to IT governance to integrate into the organisational strategy, implementations and operations.

As Posthumus and von Solms (2004) state, information security governance relates to two aspects. The first considers governance, where senior management should produce an information security policy to show the commitment towards information security and to support the organisation's objectives and the information security strategy. The second aspect is concerned with how the requirements from senior management for information security are implemented, operated and monitored in the organisation.

Information security must be treated as a top-down practise that requires the security strategy to be aligned to the organisation's business objectives and is required to cover all aspects of the organisation's processes, end-to-end from physical to technical. By following these guidelines, an organisation can develop its strategy to ensure that objectives are achieved; risk is managed appropriately; and information assets are secured and used accordingly, and to monitor and measure the status of any security programme (Hufstedler & Hancock 2006).

Organisational information that is written, printed, spoken or available in electronic form, and information handling including the creation, transport, storage and destruction of information are both elements that require safeguarding and protection (Hufstedler & Hancock 2006).

This is in contrast to IT security that is focussed on the security of information at the boundaries of technology. An example of this is confidential information that is disclosed at lunch time in a public location. Such a security incident would be beyond the scope of IT security, but from an information security perspective, security has been breached. It might be easier to buy a solution for a problem, than to change the culture of the organisation, but even a properly configured and secured system will not achieve the appropriate level of security if it is used by personnel who are unskilled or uninformed of the importance of securing this information.

The question around information security governance is a debatable one: on one hand information security is seen as an area within IT, and on the other, IT is a section in which information security has priority (Poore 2006). As per Poore, part of this depends on the role of the Chief Information Officer (CIO) in the organisation. If the CIO has responsibility to manage the information systems and technologies, then this scope lacks the requirement for information security governance.

The structure shown in Figure 1 demonstrates this point and represents the customary role of the CIO as well as the developing role of the Chief Information Security Officer (CISO). If the CIO's role is scoped to include only information systems and technologies, it will reflect a serious information security governance problem if the CISO has to report to the CIO.

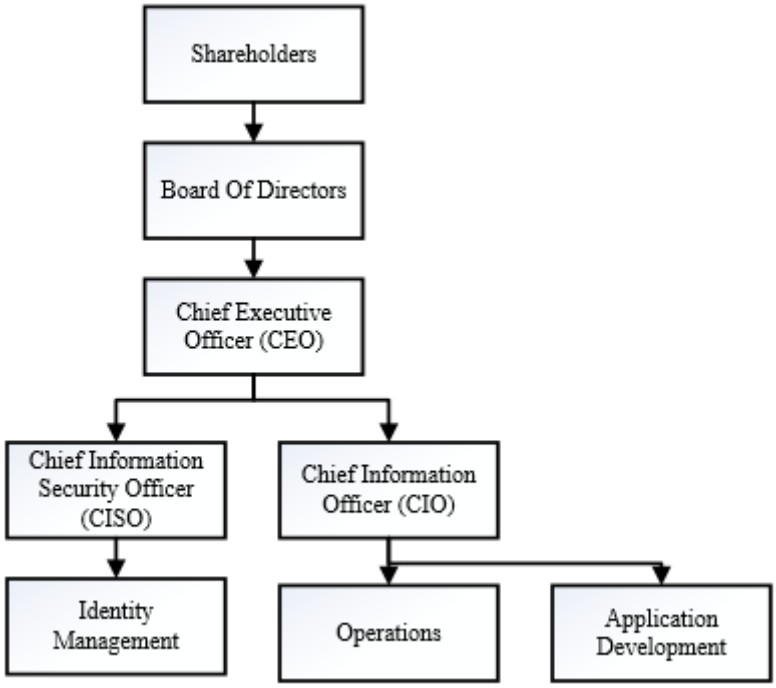

Figure 1: IT in parallel with information security [Figure 1 in (Poore 2006)]

The structure shown in Figure 2 demontrates the responsibility and scope of the CIO not only for the information systems and technologies, but also for the information assets. In this structure, the CISO does not breach information security governance by reporting to the CIO. The CIO is responsible for information processing, as well as for both information security and IT governance.

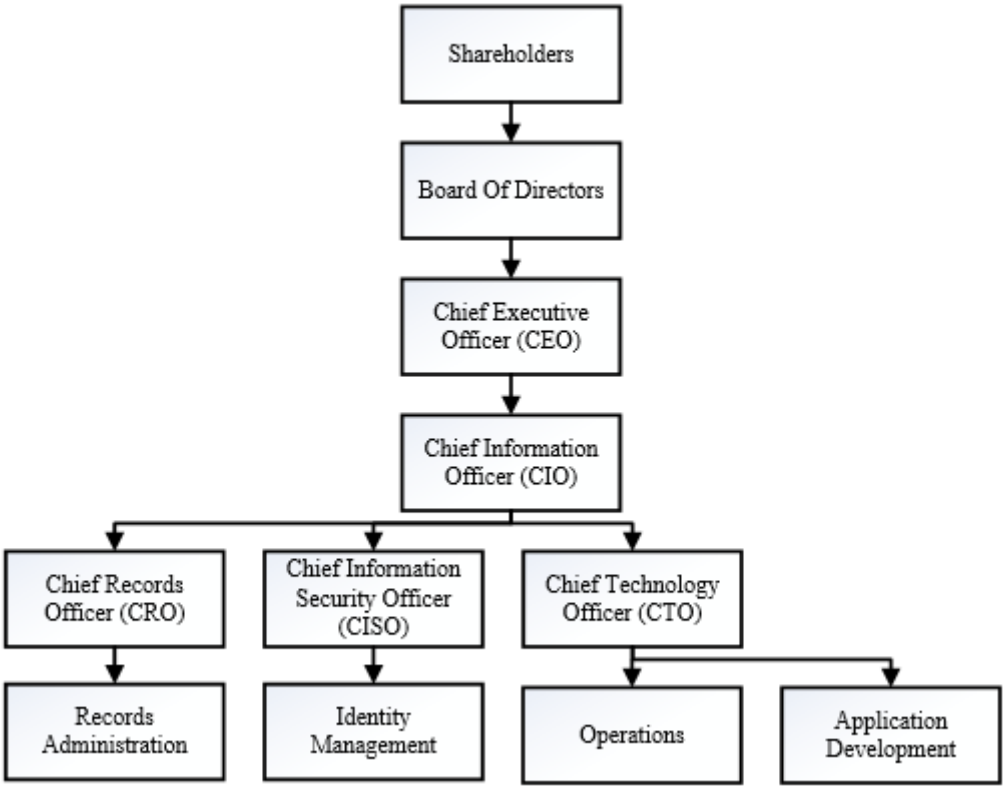

Figure 2: IT in agreement with information security [Figure 2 in (Poore 2006)]

The structure of an organisation is an important aspect in governance. Accountability in reporting structures in an organisation is a means of keeping executive management briefed as well as providing the means to keep organisational functions accountable for good information security practices (Poore 2006).

The structure shown in Figure 3 is a more complex organisational structure where information security reports through risk management and also has a dotted reporting line to the CIO who has the reponsibility for all information assets in this example. The Chief Risk Officer (CRO) also has a dotted reporting line to the Audit Committee of the Board of Directors. This is a much more complex structure, but with the essential integrated reporting, the structure provides the most probable opportunity for successful information security governance.

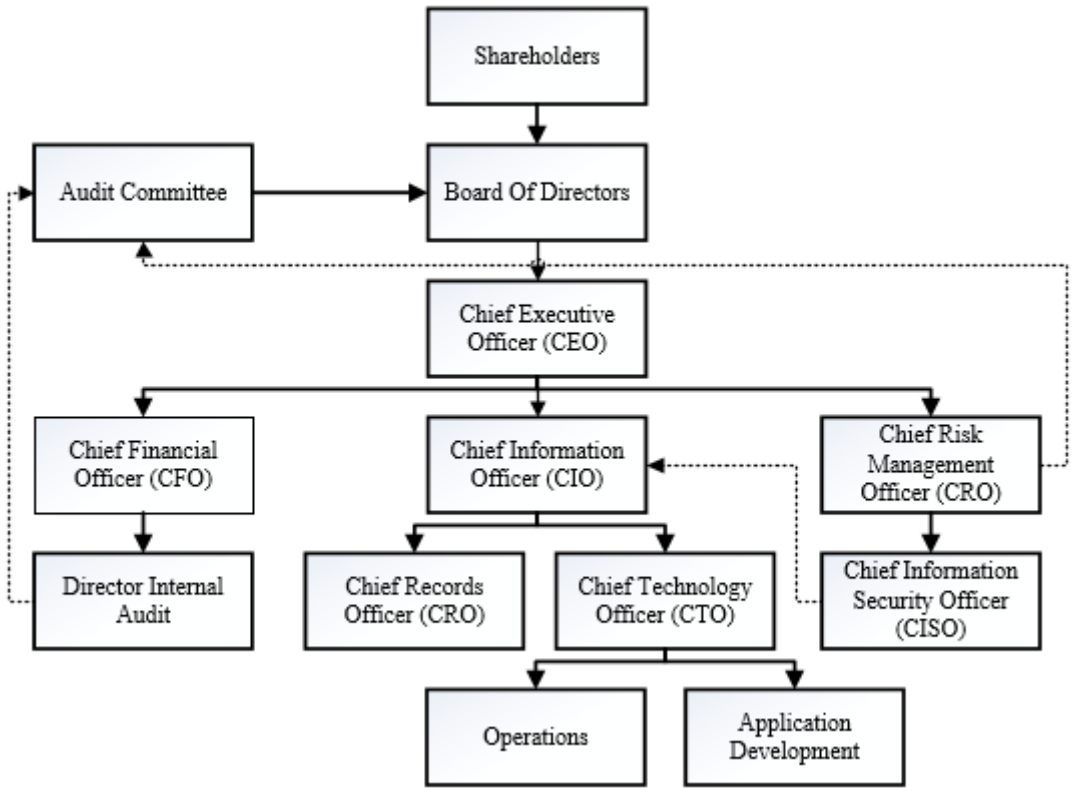

Figure 3: Complex structure for information security governance [Figure 3 in (Poore 2006)]

Apart from the organisational structure, informaiton security governance requires metrics and a way to measure them. To use traditional measurements for information security governance such as return of investment (RIO) may be challenging for a couple of reasons. To calculate the RIO of information security governance requires an understanding of the investment made and a technique to capture results such as the financial loss and gain from the investment. Information valuation methods with relevant risk management procedures may be used to quantify the value of information (Ying Chen 2005), but this still remains an intimidating task to complete successfully. From a budget perspective, information security governance is only achieved if the management of the budget reflects the organisation's requirements (Poore 2006). Similar to IT governance, to stay within budget or to go over budget is no assurance to the organisation that risk is being managed or value is being delivered.

An information security program needs to be measured to establish and provide feedback to senior management on the effectiveness thereof; this can be done by measuring elements such as the number of employees being trained in information security awareness campaigns; the reduction in information security related audit findings; or the number of information

security incidents detected and resolved. To determine the prioritisation of investments and to manage the resources of an organisation is an act of good governance (IoDSA 2009). Although budgets reflect such decisions, the corporate process associated with assigning budgets may not support good governance. Information security governance is essentially part of the foundation of an organisation especially incorporating it with the organisation's corporate governance. Although this is required for the success of information security within an organisation, information security is not always linked to the profitability it can provide to the organisation.

Organisations are required to establish a committee where the members are educated to identify and assess the need, impact, cost and benefits of information security to prioritise and cater for the businesses requirements. Such committees should have formal minutes with appropriate action items per session. Documented committee agreements can provide senior management with confirmation of due diligence and form the foundation for senior management support toward the committee's decisions and actions. This is vital to the support of an information security program in an organisation.

Organisations with structural issues can cause information security governance not to be properly enforced or to be seen as infeasible. As discussed, if the information security function is organisationally structured in IT, the focus of the function is to administer technology that is security related. This could lead to information security not being addressed in the organisation. Information security is a crucial element in overall corporate governance. Good information security governance requires a good organisational structure; cooperation across the organisation; proper metrics and prioritisation of resources. Elements such as corporate governance, regulatory, compliance and privacy programs and internal audit can assist organisations with improved information security governance.

Information security governance requires commitment from the employees to the board members to protect the organisation's sensitive information assets. Successfully managing information security governance will be of great value to an organisation (Posthumus & von Solms 2004). Information security governance is a method the organisation can use to increase business productivity and lower costs. Moreover, information security governance can produce value for several stakeholders, including corporates and governments (Posthumus & von Solms 2004).

2.4 Information Security Risk Assessment

Information security risk assessments (ISRA) enable organisations to profile and categorise information assets, and identify the security risk in order to develop effective security control strategies to treat risks (Shedden et al. 2010). ISRA offers an organisation a view of the current security state as it outlines the risk scenarios with the relevant consequences the risk could have on the organisation should the risk occur; the likelihood and rate of occurrence; possible treatment strategies; and the cost associated with the risk (Shamala et al. 2013). A problem with risk assessments though, is the process of assessing risks and using the output in such a way that the organisation will be able to define effective controls to treat those risks (Shedden et al. 2009).

The development of risk evaluation has evolved through three stages (Wright 1999). The first stage consists of a recommended checklist of information security controls a computing facility adheres to. Browne's Checklist for Computer Center Self-Audits, created by Peter S. Browne is an example of a first stage method (Wright 1999). The second stage allows organisations to identify system assets; perform threat and exposure assessments; undertake quantitative risk analysis; and establish efficient information security controls. The Annual Loss Expectancy is an example of a second stage method (Wright 1999). The third stage is closely related to the second stage, but with business impact analysis included to investigate the interrelationships between systems and document the purpose, behaviour and structure in relation to the environment the system resides in and is being used in the organisation (Craft et al. 1998). ISRA methods have progressed in the same way as the use of technology in organisations, shifting from isolated to distributed environments, and the integration of technology with the organisations operations and processes. Risk management approaches must constantly be updated as technology advances to cater for emerging risks to the organisation.

In recent research, several risk assessment methods, standards and guidelines have been proposed that differ in their objectives. Guan et al. (2013) proposed a knowledge-based information security risk assessment method in which rules are created to match assets, threats and vulnerabilities. Feng et al. (2014) proposed a security risk analysis model that can identify the casual relationship among risk factors and analyse the complexity of the spread of a vulnerability. Khanmohammadi & Houmb (2010) proposed an ISRA that focusses on business goals and the processes that support these goals to identify and assess risks based on

the role, criticality and importance of the goal for the organisation, rather than focussing on assets. Shedden et al. (2011) did similar research to investigate how ISRA methods can recognise and manage the risk associated with business goals and processes.

There are several different types of information security risk management methods, including those designed by international organisations such as the National Institute of Standards and Technology publications (NIST 2012; NIST 2010; NIST 2011), and the ISO/IEC publications (IEC 31010 2009; ISO/IEC 27005 2011). There are also information security risk management methods available from professional organisations such as the Risk Analysis and Management Method (Yazar 2012), the CORAS approach (Lund et al. 2011), the OCTAVE approach (Panda 2009), and Microsoft's Security Risk Management Guide (Dillard et al. 2006).

The shared objectives between the different ISRA methods are to list and prioritise enterprise risk and to propose appropriate mitigation steps to manage enterprise risk at an acceptable level. An organisation's information system is subject to severe threats that can have a negative impact on the organisation by affecting employees, operations, business processes or assets by exploiting vulnerabilities with the aim to compromise the confidentiality, integrity, and availability of the information stored, processed or transmitted from the systems (NIST 2012). It is therefore important that an organisation's board and management understand their accountably and responsibilities towards the management of information security risk related to the utilisation and operation of information systems that support critical business functions and processes.

2.5 Information Security Management: Compliance vs. Operation

As information security governance is being incorporated in corporate and IT governance (Posthumus & von Solms 2004), so the traditional role of information security management should evolve into a more established function that is responsible for all aspects of information security in an organisation. With the growing usage of the Internet and social media (InternetWorldStats 2012), new risks are introduced to organisations and controls such as policies and standards are created and enforced to ensure that IT is being utilised in a controlled and secure manner. Internationally accepted best practises and standards stress the importance of such controls for proper information security management, which has proved

necessary for good corporate and IT governance within organisations (COBIT 2012; ISO/IEC 27001 2005).

Enforcing and complying with governance controls such as policies and standards has become just as important as the enforcement of technical security controls throughout an organisation. Information security management covers operational information security management as well as a portion of information security governance such as the creation of policies, standards and procedures. Good information security governance requires the aspect of compliance enforcement and monitoring in organisations, but as per Von Solms (2005) this has not yet formed part of the customary information security management role. With this in mind, information security governance should consist of a separation between information security compliance and operational management within an organisation.

Information security operational management has always been a well-defined and understood dimension of information security governance and should consist of, but not be limited to, technical activities such as (Von Solms 2005):

- Logical access management, i.e., system and application account management;
- Network security management, i.e., network segregations and securing of networks using firewalls;
- Malicious code management, i.e., management of anti-virus and virus related incidents;
- Vulnerability and patch management, i.e., the configuration and scheduling of vulnerability scans on the network and deployment of latest released security patches;
- Backup and restoration management, i.e., ensuring backups of systems and the securing thereof.

These actions are important to ensure that organisations' information assets are protected from risks and that the confidentiality, integrity, and availability of these assets are not compromised. Traditionally, organisations considered such actions to be the responsibility of information security management; however, this creates the impression that information security is a technical activity that is performed by a technical unit (Von Solms 2005). The representation of information security management has changed though, and now includes non-technical activities such as (Von Solms 2005):

- Information security documentation frameworks, i.e., the creation of information security policies, standards, procedures, processes and baselines;
- The enforcement of compliance towards the information security documentation framework, and the ability to identify and manage risks;
- The creation and launch of information security awareness campaigns to educate peers and the rest of the organisation on everyday good information security practices, such as password usage.

The technical as well as non-technical activities complement the general understanding and acceptance of information security management in organisations. The enforcement and measurement of information security compliance, and the ability to identify and manage information security risks are essential elements of good information security governance, which links back to IT and corporate governance.

In all industries, including information security, it is a generally accepted truth that a policy that is not enforced is not worth the paper it is written on. It is essential that compliance be measured and enforced, and risks be identified, reported and managed for good governance. The role of measuring and enforcing compliance within information security governance has become an essential aspect of IT risk management in an organisation (Von Solms 2005). Organisations carry out audit functions to be able to identify areas of risk in the IT environments as well as report the level of compliance an organisation adheres to according to policies, standards and procedures on an annual basis (Basel 2010). With the dependency of information systems in organisations for day-to-day business, the daily activity of monitoring and enforcement of compliance is pivotal. Compliance activities that should be managed include but are not limited to (Von Solms 2005):

- Information security documentation frameworks, i.e., the completeness, effectiveness, review, approval and availability of policies, standards, procedures, processes and baselines;
- Risk management, i.e., the measurement of the effectiveness of risk identification and mitigation;
- Information security awareness, i.e., the measurement of the effectiveness of the information security awareness program;
- Compliance with national requirements such as regulations and legislations.

Items identified in activities such as these are required to be reported to the board of directors and senior management of an organisation allowing them to endorse and perform their responsibility towards good governance. Separation of duties is a control used to separate and distribute the responsibilities so that a single employee does not have the ability of weakening or disrupting a critical business function (Swanson & Guttman 1996). An example of separation of duties in an organisation is the separation of internal audit and IT, this way the internal audit department can act independently and objectively towards assessments done on the IT department. This principle should effectively be enforced between information security compliance management and information security operations management, as information security operations should not be measuring their own compliance towards organisational policies and standards, as well as the level of risk identification and mitigation, as this could lead to a false perception of the current state of the environment.

Von Solms (2005) argues that information security governance needs to be divided into two separate units: information security compliance management and information security operations management. To align this with IT and corporate governance, independent and objective monitoring, measurement, and reporting on a level at which IT and information security risks are identified, managed, mitigated and reported on, is essential to an organisation.

2.6 Information Security Compliance and Frameworks

Based on the research done by Von Solms (2005), it is clear that the enforcement and compliance of information security is a critical aspect of corporate and technology governance within an organisation. Organisations need to ensure that policies are enforced and the compliance from both employees and the technical aspects are monitored and measured. The compliance approach of information security evolved from focussing only on the technical requirements to a broader approach that included business requirements and processes (Saint-Germain 2005). This approach created awareness of the importance of information assets and the protection thereof leading to more interest and investment in security management frameworks by organisations.

As per Arnason and Willet (2007), security management frameworks have been developed to identify information security risks and to manage information security accordingly. Such a framework enhances the information security posture of an organisation by enabling the

identification and severity of an information security breach, and the response to one. The components of information security require a combination of elements including people, processes and technology (Hufstedler & Hancock 2006). Veiga & Eloff (2007) indicated that technical controls such as a firewall or anti-virus program, are not sufficient nor capable of securing information assets alone. They motivated this by stating that actions such as awareness campaigns and processes such as password management, together with technical controls are required to mitigate risk and protect sensitive organisational data.

Tshinu et al. (2008) indicated that organisations such as the South African banking industry rely on information and communication technology management frameworks. In such cases, methods need to be developed that will combine industry best practices with business objectives as found in information security frameworks (ISO/IEC 27001 2013). The summary of the findings though showed that there was limited reference to the ISO/IEC 27001 standard from the banking organisations that were part of the study. Members of the banking Information Security Forum found it easier to use the Standard of Good Practice for Information Security (ISF 2013), but customised it with reference to the ISO/IEC 27001 standard for internal usage.

Security management frameworks need to be defined to cater for the specific needs of an organisation. There are a variety of information security standards organisations can choose from to fit their requirements. Such standards include standards from ISO[6], Institute of Electrical and Electronics Engineers[7], and the National Institute of Standards and Technology[8] (NIST). The ISO/IEC 27001 standard is one of the most used and referenced information security frameworks globally. It has been accepted as a national standard that organisations are required to comply with in several countries such as Finland, Sweden, the Netherlands, Norway, and Spain (Saint-Germain 2005).

The requirements for an information security framework are increasing as these provide the confidence in the capability of an organisation to secure information in their possession. All elements of information security are required to be implemented to provide a suitable level of protection within an organisation. With the adoption of an information security framework, and the support and drive from senior management, organisations will be able to develop security measures to mitigate identified information security risks.

[6] www.iso.org
[7] www.ieee.org
[8] www.nist.gov

2.7 Summary

In this chapter, we discussed the relation between corporate, IT, and information security governance with the aim of providing an overview and emphasising the differences between them and the role each plays within an organisation. The chapter also provided an overview of information security risk management, information security management, and information security compliance and frameworks to provide the reader with more clarity on these areas.

Chapter 3: Information Security Standard

This chapter provides a review of the literature relating to ISO/IEC 27001, with a focus on investigating the adoption of ISO/IEC 27001 in South Africa. Although the standard was available, it was not a requirement of any of the South African regulations in recent years, making it reasonable to propose that the literature dedicated in this context is restricted. Consequently, there has been limited adoption of the standard in South African organisations owing to the absence of government enforcement of the security framework, as well as the challenges that are associated with the use of the standard. This chapter considers these issues, as well as the risks that are associated with the management of information security. A detailed overview of the ISO/IEC 27001 standard is presented followed by some of the alleged benefits that the standard provides organisations and the challenges related to the adoption thereof.

3.1 History and Timeline of the ISO Information Security Standards

The focus of separating and managing information security from IT security slowly became known through the industry. Changes started to occur with the initial release of the "*Information Security Policy Manual*" that was originally developed by The Royal Dutch/Shell Group in the 1980's (Kouns & Minoli 2011). The UK Department of Trade and Industry (DTI) established the Commercial Computer Security Centre (CCSC) in 1987 and developed and published the "*DTI CCSC User's Code of Practice*" in 1989 based to a degree on the Royal Dutch/Shell Group's "*Information Security Policy Manual*" (Van Bon 2006). The DTI's publication later became the foundation for the British Standard (BS) 7799 Information Security Management Standard and was published by the British Standards Institute (BSI) in 1995 (DTI 2000), focussing not just on IT, but information security related to people, processes and information (BS 7799-1 1999).

The first revision BS 7799:1999 (BS 7799-1 1999) followed by an extended revision that consisted of consultation from the public, was released as a two-part standard, with part one as BS 7799-1 (BS 7799-1 1999), and part two as BS 7799-2 (BS 7799-2 1999) in 1999. Part one provided direction on best practice of information security management and was titled "*Code of Practice for Information Security Management*". Part two provided the specifications that an organisation's ISMS could be measured, monitored and benchmarked on the implementation of part one for certification and was entitled "*Specification for*

Information Security Management Systems". The two standards are linked through Annex A of the BS 7799-2 standard that lists the information security controls organisations aligning to the standard are required to consider when implementing an ISMS. The BS 7799-2 standard's Annex A list of information security controls are aligned to the BS 7799-1 standard controls. The BS 7799-2 standard provides organisations with guidance on how to implement the controls listed in the BS 7799-1 standard (Calder 2009).

The BS 7799-1:1999 standard was adopted by the ISO on a "*fast track*" process in 1999, and was published by the ISO/IEC Joint Technical Committee as ISO/IEC 17799:2000 in December 2000 (Kouns & Minoli 2011). The subsequent extended revision of ISO/IEC 17799:2000 consisted of another consultation phase, and was re-published in October 2005 as ISO/IEC 17799:2005. The ISO/IEC 17799:2005 standard then went through a name change in July 2007 to ISO/IEC 27002:2005 (Arnason & Willett 2007). The latest revision published by the ISO/IEC committee is ISO/IEC 27002:2013, which replaced the ISO/IEC 27002:2005 standard (ISO/IEC 27002 2013).

The BS 7799-2:1999 was reviewed and published in September 2002 as BS 7799-2:2002 (BS 7799-2 2002), and focussed on ISMSs, rather than just security controls. National standard bodies around the world in countries such as Sweden, Netherlands, Ireland and Finland, adopted the BS 7799-2:2002 standard and re-published it as a National Standard (Calder 2009). Spain as an example, adopted the BS 7799-2:2002 standard and developed and published a local version as UNE 71502:2004 (AENOR 2004). The Australian and New Zealand Standards bodies, joined forces and published their version of AS/NZS 7799.2:2003 in February 2003 (AS/NZS 7799.2 2003). Later, the BS 7799-2:2002 standard was adopted by ISO, revised, and published as ISO/IEC 27001:2005 in October 2005 (ISO/IEC 27001 2005). The latest revision published by the ISO/IEC committee is ISO/IEC 27001:2013, which replaced the ISO/IEC 27001:2005 standard (ISO/IEC 27001 2013).

From a South African perspective, the South African National Standards (SANS) body, the South African Bureau of Standards (SABS) adopted the BS 7799-2:2002 as well as the ISO/IEC 17799:2000 (ISO/IEC 17799 2000) standards. Both were re-published as a local version SABS 7799/2, which was subsequently replaced by SANS 27001:2006, and SABS 17799, which was subsequently replaced by SANS 27002:2008 (SABS 2014b). Figure 4 illustrates the stages in the development of these core standards.

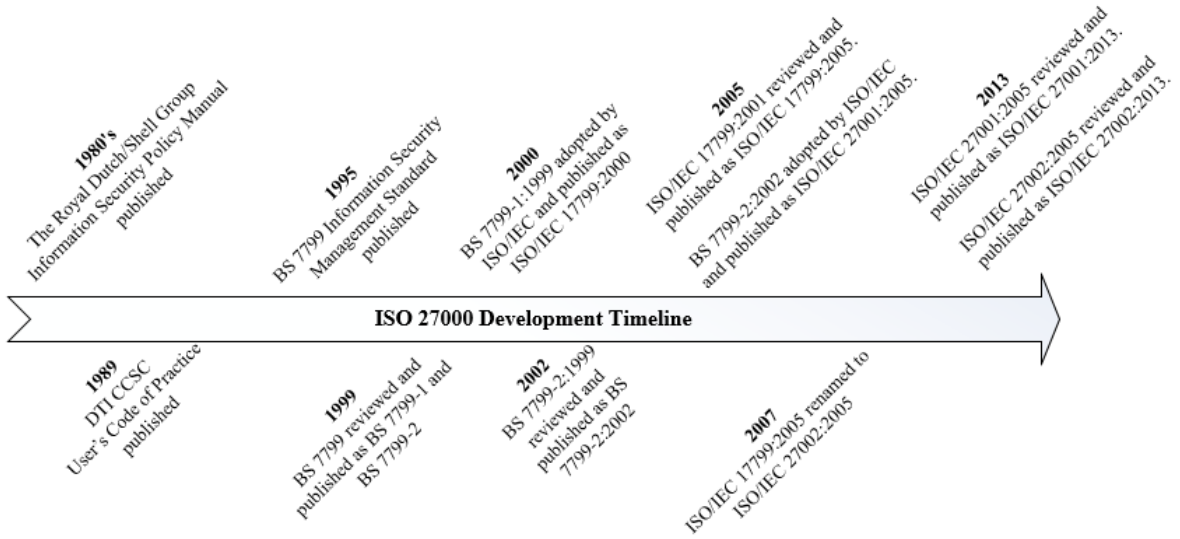

Figure 4: ISO 27000 development timeline [Figure 4 from (ISECT 2014)]

3.2 Overview of ISO/IEC 27001

Several information security frameworks exist to assist organisations to identify and assess information security risks, implement controls to mitigate such risks, comply with governance requirements as well as regulations specific to privacy and information security. Of the various frameworks available, the most comprehensive method is the adoption, implementation and certification of an internationally known and utilised information security management framework.

The ISO and IEC, drive the system for international standardisation. National members of these organisations are involved in the development and establishment of internationally recognised standards. The ISO 27000 series provides best practice recommendations on information security management, risk management, and control management relevant to an ISMS. Figure 5 provides a list, together with a brief description of the ISMS related published standards in the ISO 27000 series.

The ISO/IEC 27001 standard titled "*Information Technology – Security Techniques - Information Security Management Systems –Requirements*" is an internationally recognised information security standard. The standard formalises and models the requirements for the development as well as the operation and management of an ISMS. The goal of ISO/IEC 27001 is to provide a consistent and integrated implementation, operation and management of an ISMS with various other management standards such as ISO 14000 that addresses

Environmental Management (ISO 14000 2004), ISO 9000 that addresses Quality Management (ISO 9000 2008), and ISO 31000 that addresses Risk Management (ISO 31000 2009).

The ISO/IEC 27001 standard provides guidance to organisations to protect their sensitive information against the loss of confidentiality, integrity, and availability by applying a risk management process that provides surety and confidence that risks to the organisation are managed accordingly. The ISO/IEC 27001 standard from a business risk approach describes the ISMS as a management system to establish, implement, monitor, manage and continuously improve an ISMS (ISO/IEC 27001 2005).

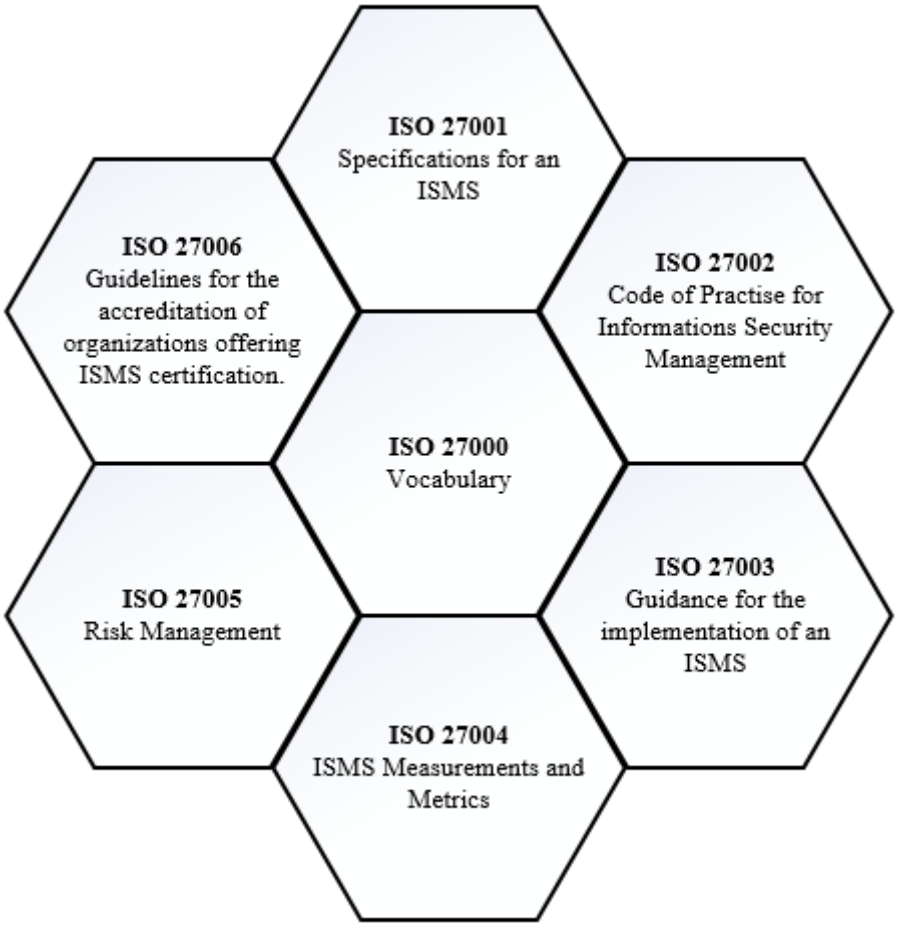

Figure 5: ISO 27000 series related to ISMS [Figure from (ISO)*]*

The adoption of the standard is a strategic decision for an organisation, as the establishment and implementation of an ISMS is motivated by the needs and objectives of an organisation. The ISO/IEC 27001 standard provides organisations with the ability to implement an ISMS that will address all the information security aspects of an organisation, from the organisation

structure, senior management responsibilities, resource management, to policies and procedures and processes (ISO/IEC 27001 2005). With such an ISMS in place, organisations will have the ability to manage information security while reducing risk to the business.

The structure of the ISO/IEC 27001:2013 standard consists of the following clauses. Clause 4 to 10 are mandatory requirements for the implementation and certification of ISO/IEC 27001:2013 as shown in Table 1 (ISO/IEC 27001 2013).

Table 1: ISO/IEC 27001:2013 clauses

Clause 0	Introduction
Clause 1	Scope
Clause 2	Normative references
Clause 3	Terms and definitions
Clause 4	Context of the organisation
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance evaluation
Clause 10	Improvement
Annex A	Objectives and controls

ISO/IEC 27001:2013 Annex A consists of 14 control areas. These control areas provide information security controls for all areas of an organisation, that is, legal, managerial, organisational, operational and technical. The control areas consist of 34 control objectives that are statements of the security goals for each of the 14 control areas. The standard includes 114 controls that identify the means for satisfying the control objectives. The structure of the standard uses a top-down approach with a drive from the senior management level down to the technical and operational levels of an organisation.

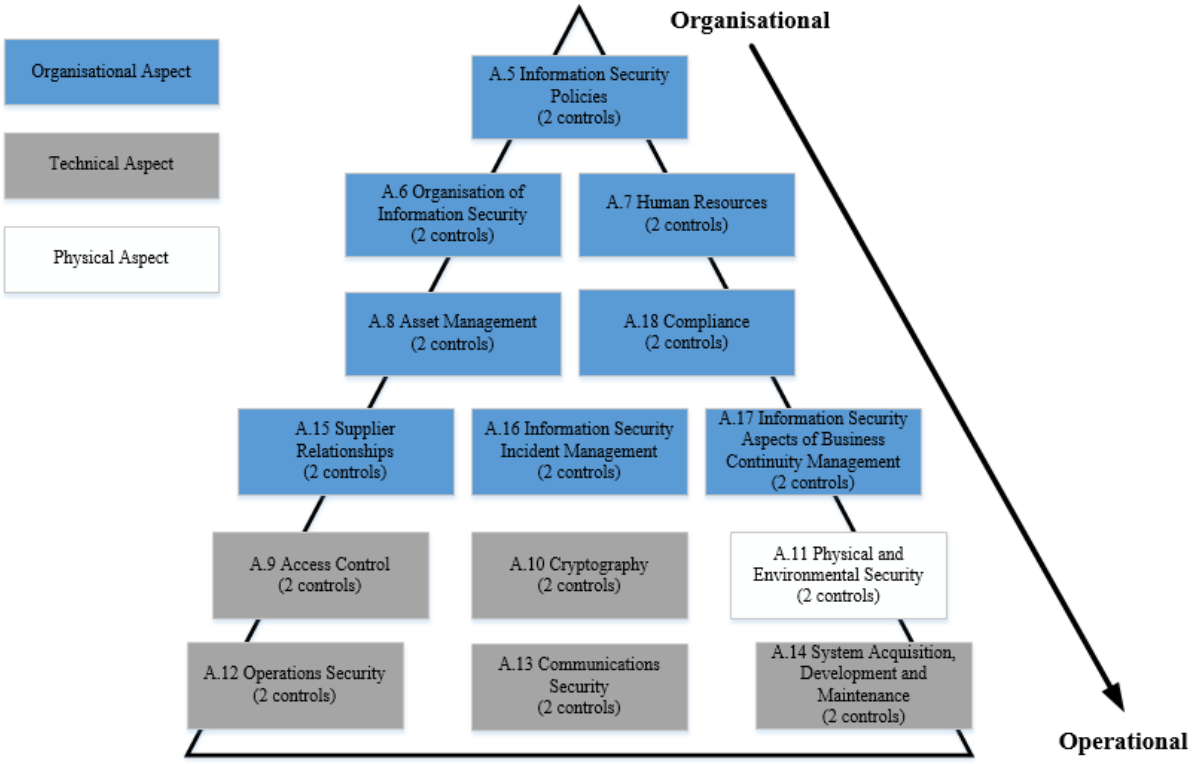

Figure 6: ISO 27001 control areas [Figure 6 in (Saint-Germain 2005)]

An ISMS provides organisations with the ability to use a systematic approach to protect sensitive information as it involves procedures, processes, employees, and information systems. Moreover, an ISMS ensures protection on multiple initiatives within a corporate strategy and ensures that all efforts are co-ordinated to provide optimal protection of sensitive information. A management system must therefore provide the means for planning, developing, evaluating, setting controls, and documenting. For organisations to function effectively, activities that use resources and are able to manage the transformation from an activity item to a result can be considered as a process (AS/NZS 7799.2 2003). A "*process approach*" is described as the management of processes including the interaction of the processes (AS/NZS 7799.2 2003). Organisations adopting a process approach provide awareness and encourage their employees to emphasise the importance of the business' understanding of information security; the establishment and enforcement of an information security policy; the management of information security risks; and the management and continuous improvement of an ISMS within the organisation (AS/NZS 7799.2 2003).

This is the foundation of the ISO/IEC 27001 Plan-Do-Check-Act (PDCA) model that aligns to the ISO 9001 Quality Management model (ISO 9000 2008), which can be applied to all

known ISMS processes. The details of the PDCA model are described in Table 2 (ISO/IEC 27001 2005):

Table 2: Plan-Do-Check-Act model [Table 2 from (Saint-Germain 2005)]

PLAN *Establish the ISMS*	* Identify business objectives * Establish senior managing support * Define the ISMS scope and policy * Initiate risk assessment and report * Select control objectives * Prepare the SOA
DO *Implement and operate the ISMS*	* Formulate the risk treatment plan * Implement the SOA controls to meet the control objectives
CHECK *Monitor and review the ISMS*	* Execute monitoring procedures for controls * Review the level of risk (acceptable and residual) * Measure the effectiveness of the ISMS; * Conduct internal ISMS audit
ACT *Maintain and improve the ISMS*	* Conduct corrective and preventive assessments * Implement ISMS improvements * Validate improvements * Maintain communication with relevant stakeholders

Figure 7 illustrates the ISMS development, maintenance and improvement cycle that uses the PDCA model. The PDCA is a process approach model that is the primary model of the ISO/IEC 27001 standard and provide organisations with the ability to maintain, manage and improve the information security posture (ISO/IEC 27001 2005). The PDCA model is a continuous improvement cycle as the ISMS is regularly monitored and the controls are measured to confirm if risks to the organisation are managed appropriately. If such controls are not effective, mitigating controls need to be established and implemented.

The release of the latest version ISO/IEC 27001:2013 brought some changes to the standard. Whereas the PDCA model was an explicit section in the ISO/IEC 27001:2005 version, the

ISO/IEC 27001:2013 requires continuous improvement throughout the mandatory clauses of the standard, and highlights the importance of measuring and assessing the performance of and ISMS in an organisation (BSI 2013). Organisations now have the option of using different models besides the PDCA model as their approach for continuous improvement.

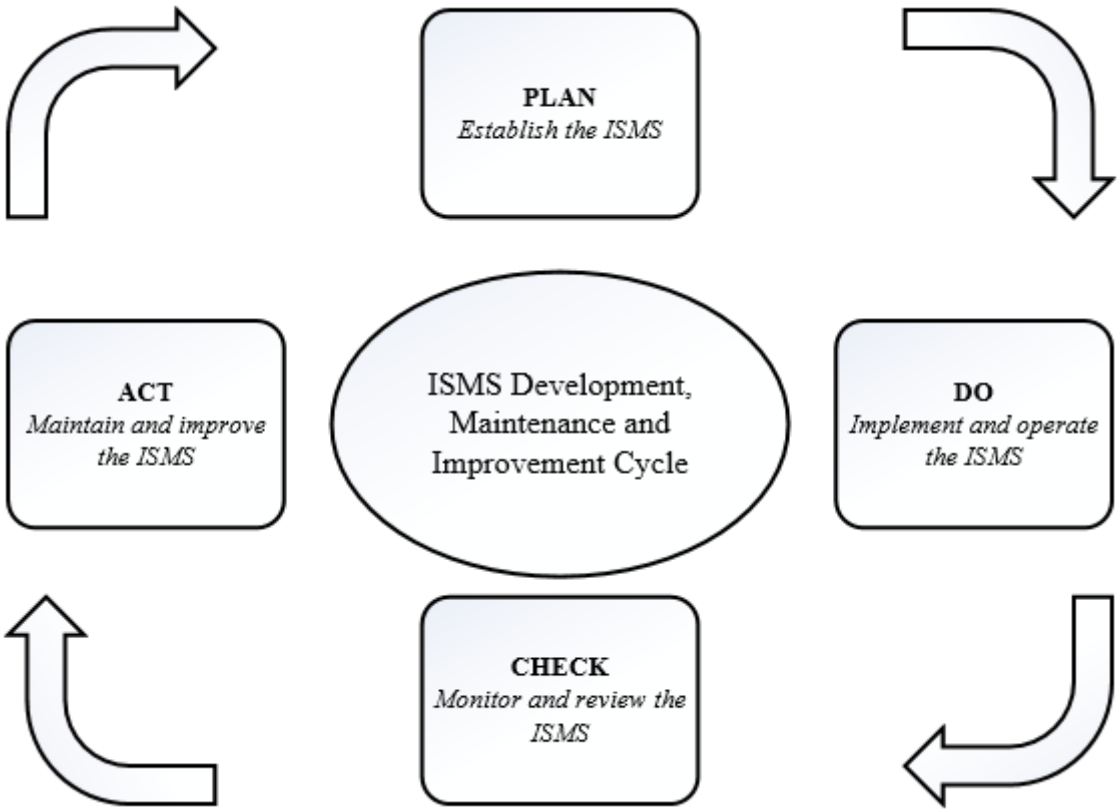

Figure 7: ISMS cycle [Figure 7 from (ISO/IEC 27001 2005)]

The standard is a model for establishing, implementing, monitoring and improving an ISMS (ISO/IEC 27001 2013). The model is internationally understood, and can be adopted across the globe and in any environment (including hardware and software). The standard has several positive aspects such as, it is technology neutral, consistent, comprehensive and consists of best practices. It has been designed to be flexible and covers a diverse range of organisational sectors (government agencies, financial institutes, telecommunications, non-profit organisations), and any size organisation (small, medium, enterprise) (ISO 2012). It consists of security control measures that organisations can use to mitigate information security risks. Organisations that strive for information security governance, are required to establish the primary objective of information security within the organisation and amend the use of the standard accordingly to these objectives to provide optimum value.

Although flexible, organisations still need to manage the implementation of the standard effectively as it touches on several aspects of information security in an organisation. As per the paper of Saint-Germain (2005), Table 3 gives an overview of the uses of the ISO/IEC 27001 standard in various sized organisations.

Table 3: ISO/IEC 27001 objectives in organisations [Table 3 from (Saint-Germain 2005)]

Organisation size	**Organisation's objectives in using the standard**	**How the standard can be used to accomplish the objective**
Small Organisations *Fewer than 200 employees*	The objective of smaller organisations is to raise information security awareness to management	The standard contains information security awareness controls
Medium Organisations *Fewer than 2000 employees*	The objective of medium size organisations is to create corporate culture of information security compliance	The standard contains controls required to create an information security policy
Large Organisations *More than 2000 employees*	The objective of larger organisations is to implement and certify in the standard	Organisations use the standard to plan, implement, monitor and improve an ISMS

3.3ISO/IEC 27001 ISMS Processes

The focus of the research done by Humphreys (2008) was to identify what international standards such as the ISO/IEC 27001 standard, have to offer organisations, the benefits an organisation can gain from the standard, as well as how the standard assists organisations with compliance. The ISO/IEC 27001 standard adopts the process approach from the establishment to the continuous improvement of the effectiveness of an ISMS that can be used to identify and mitigate threats to an organisation (ISO/IEC 27001 2013). Such processes include risk management, measurement, monitoring, review and improvement.

3.3.1 ISMS Risk Management Process

A key aspect of governance in organisations is to be able to identify and manage risks accordingly. An organisation needs to know the risks they face to be able to create an effective approach to ultimately protect the information resources of the organisation. The ISO/IEC 27001:2013 risk assessment and treatment processes align to the principles and guidelines stipulated in the ISO 31000 standard (ISO 31000 2009). The ISO/IEC 27001 risk management approach requires organisations to adhere to the following processes (ISO/IEC 27001 2013):

The information security risk assessment process must:

- Establish and document a risk assessment process;
- Ensure that assessments are initiated at planned intervals or when major changes occur, are consistent, provide value and can be compared;
- Be able to identify information security risks;
- Be able to analyse information security risks;
- Be able to evaluate information security risks;
- Retain the documented information of the results of the risk assessments.

The information security risk treatment process:

- Defines, applies and documents a risk treatment process;
- Using the risk assessment results, selects appropriate risk treatment options;
- Determines which controls are required to implement the risk treatment options;
- Compares these controls with Annex A to determine that no required controls are absent;
- Formulates the risk treatment plan;
- Obtains approval from the risk owners of the risk treatment plan as well as the acceptance of the residual risks.
- Retains the documented information of the results of the risk treatment.

Once information security risks to the organisations have been identified, the risks are recorded in a risk register, and prioritised in order of type and severity. Additional details of the risks are completed together with the estimated impact the risk could have on the

organisation, and details that can be used to create a risk profile. The next step is to define the treatment options for the identified risks. The ISO/IEC 27001:2013 version shifts the importance of the effectiveness of the controls to the effectiveness of the risk treatment plan. ISO/IEC 27001 provides four information security risk treatment options (ISO/IEC 27001 2013):

- Risk acceptance – knowingly accepting the risk
- Risk avoidance – avoiding the activity that caused the risk
- Risk transfer – transfer to insurance or contracting out of the risk
- Risk reduction – implement controls to reduce the risk

Management needs to decide what the best treatment option would be for each identified information security risk by considering the impact, costs and the benefit of implementing security measures required to mitigate the risk compared to not taking any action against the risk. The decision from management should be a case of mitigating information security risks, and increasing the information security investment in the organisation (Hufstedler & Hancock 2006). Whatever risk treatment option management decides on, a portion of risk (known as residual risk) will not be able to be reduced to nil (Humphreys 2008). Once management has selected and agreed on the controls to mitigate the information security risk, the controls need to be implemented and used in practice. The implementation of the controls will require the assignment of roles and responsibilities for those resources who are assigned control related tasks, as well as relevant awareness and training.

The last section in the risk management process is to assess the effectiveness of the implemented control and to monitor and review the information security risks. This is vital as daily operations and changes may affect the risk profile of the organisation. Changes must be monitored and the risks must be reassessed to ensure controls remain effective.

3.3.2 ISMS Measurement, Monitor and Review Processes

The establishment of measuring, monitoring and reviewing processes are important to an organisation to enable them to assess the ISMS security measures implemented to protect the organisation's information assets (Humphreys 2008). An example would be to measure the effectiveness of an information security awareness campaign that was launched to provide awareness and education to employees around the organisation's information security policy. The measurement involves measuring the effectiveness of the rollout of the campaign to all

of the organisation's employees, and the acceptance of the information security policy by staff members. The monitoring and review process will be used to review the results of the measurements.

The monitor and review process can also be used to monitor and review actions such as risk reassessment reports, internal audit activities and reports, as well as the compliance and use of procedures by employees (Humphreys 2008). It is vital that organisations are able to monitor and review changes in the business environment that could have an impact on the organisation's productivity as changes can hamper the organisation's ability to safeguard its information assets and create instabilities in the risk profile. Changes must be monitored and reviewed and assessed to what level they influence the organisation's risk profile. This provides the organisation with the ability to avoid various threats it may be challenged with.

3.3.3 ISMS Improvement Process

The results of the ongoing activity of the measuring process and the monitor and review process can be used as recommendations for improvements to an organisation's ISMS that will lead to the implementation and modification of security controls. These recommendations are the after effect of a change in the organisation's risk profile. One of the key success drivers of the ISO/IEC 27001 standard is that it enhances the information security posture by enforcing a cycle of continual improvement.

3.4 ISO/IEC 27001 ISMS Implementation

ISO/IEC 27003:2010, titled "*Information technology -- Security techniques -- Information security management system implementation guidance*" is a standard that was designed to assist organisations with the implementation of an ISMS in accordance with ISO/IEC 27001:2005 (ISO/IEC 27003 2010). The standard covers the preparation and planning of activities prior to the actual implementation thereof. It describes the specification and design of the ISMS which involves obtaining senior management support, commitment and approval; defining the scope and the limitations; risk assessment and treatment plans; designing the ISMS and planning the implementation project plan. Implementing an ISMS in an organisation consists of five steps (ISO/IEC 27003 2010). Table 4 presents an overview of these steps with a brief description of each as per ISO/IEC 27003 (ISO/IEC 27003 2010).

Table 4: ISO 27001 implementation steps

1	**Senior Management Approval**	Obtain senior management support, commitment and approval towards the ISMS implementation by defining a business case and project plan.
2	**Defining the ISMS**	Define the ISMS scope and the limits of the ISMS implementation. Development of the information security policy.
3	**Requirements Analysis**	Define requirements to support the ISMS. Identify information assets within ISMS scope. Conduct an information security assessment.
4	**Risk Assessment and Risk Treatment**	Define risk methodology and conduct risk assessment. Define and select controls from Statement of Applicability (SOA) for risk treatment. Obtain management approval for control implementation.
5	**Designing the ISMS**	Designing of organisational security based on selected risk treatment options; physical and organisational processes; designing the ISMS requirements. Produce final ISMS project plan.

The ISO/IEC 27003 version 2010 standard was designed to cater for the ISO/IEC 27001:2005 version. The revised ISO/IEC 27003 standard will be updated to re-align to the 2013 version of ISO/IEC 27001 with focus on the management system, rather than the management of the information security controls.

3.4.1 Senior Management Approval

As per the benefits discussed in the ISO/IEC 27001 Information Security Research Report Summary, 93% of the organisations that participated in the report, considered the endorsement of senior management as a key factor for the establishment, implementation and maintenance of an ISMS in an organisation (BSI 2012). To acquire the backing of senior management, a business case that includes the objectives and the priorities of the implementation of an ISMS as well as the structure of the organisation for the ISMS is required. The objective to implement an ISMS within an organisation should reflect the organisation's approach to manage information security, and should be included in the organisation's strategic objectives; review of management systems already implemented; and

the legal and regulatory requirements that are applicable to the organisation (ISO/IEC 27003 2010). Senior management needs to understand the business case of an ISMS implementation project in order to make systematic decisions that will ultimately have an impact on an ISMS. This will enable an organisation to understand the relevance of the ISMS, as well as assist in identifying and assigning the roles and responsibilities that are required for the project.

Senior management approval towards an ISMS project can provide much more value than just information security compliance (Kosutic 2014). Senior management is required to approve, and amend the ISMS budget when required; review whether the ISMS fulfils the outlined objectives; amend the ISMS scope if needed; discuss and agree on improvements required for the ISMS; assign resources to the project; and modify organisational wide documents such as policies and procedures. Management review can also provide awareness of information security to the senior management team. Senior management approval for the implementation of an ISMS is crucial when deploying information security throughout an organisation.

3.4.2 ISMS Scope

The objective of the ISO/IEC 27001 standard is to implement an ISMS throughout an organisation, thereby providing assurance that the majority of the organisation's information security risks are being identified and managed accordingly. The standard does however, provide the option of scoping such an implementation to a specific business unit or requirement. Defining the ISMS scope is the first step in the entire process of defining the ISMS. The amount of effort required to implement an ISMS is dependent on the extent of the scope to which it is applied. Limiting the scope of an ISMS can assist organisations in cost saving as the implementation size decreases, but this raises different problems as it provides overhead to the implementation (Kosutic 2010). If an ISMS scope is not the entire organisation, and it only focusses on a single department, this means that all the areas outside of that department are seen as external to the scope. From a certification body's perspective, any area that is excluded in the scope, irrespective whether it is an internal department or an external supplier, will be treated as an external party in the assessment. This in turn creates overhead where the department in scope is required to initiate risk assessments and agree on terms and conditions of service delivery with internal departments that are not in the scope.

For organisations that are pursuing certification of the implementation, it is vital for senior management to define the scope and limitations as well as to provide a documented ISMS

scope that includes the justification for exclusions as this is a mandatory requirement for certification (ISO/IEC 27002 2013). When defining the ISMS scope, senior management needs to decide to what level the scope will extend within the organisation. Decreasing the ISMS scope may assist in cost saving, but increasing the scope to cover the entire organisation provides more value and less overhead of the implementation as well as certification of an ISMS within an organisation.

3.4.3 ISMS Statement of Applicability

The ISMS statement of applicability (SOA) is the core document that defines how the security measures of an ISMS will be implemented. The SOA document is the link between the risk assessment and the security measures selected to mitigate those risks. The objective of the SOA document is to define which security controls from Annex A will be implemented to mitigate the identified information security risks. It also includes the status of the selected controls as well as the security measures that have not been selected, with justification for their exclusion.

The SOA needs to be organised according to the ISO/IEC 27002 standard and any other requirements need to be mapped to the ISO/IEC 27002 standard if an organisation decides to adhere to ISO/IEC 27001. The security controls from the ISO/IEC 27002 standard can be referenced as a checklist in Annex A to avoid overlooking necessary controls. Organisations do however, have the option to use a custom approach, or even use a different framework such as the National Institute of Standards and Technology (NIST) SP800-55 (Chew et al. 2008) or COBIT (COBIT 2012) as a reference point for the relevant security controls. The SOA should document the following for each security control (Siig 2013):

- the source from which the security requirement originated;
- the level of compliance of the selected security measure;
- a justification of the selection of the security measure OR the reason why the control was not selected;
- a description of the security measure.

After the security measures have been selected, the next step is to write the SOA document. Using a structured tool such as a spreadsheet or database is recommended as this facilitates working with the content of the SOA as well as provides capabilities such as sort and filter based on parameters such as compliance levels or sources. For ISO/IEC 27001 certification,

auditors use the approved ISMS SOA as their central document for their assessment, and work through the selected controls to ensure that the security measures have been implemented as stated in the SOA. With the recent release of the revised ISO 27001 2013 version, the main difference between the versions, Annex A, has been updated to reflect the security controls stated in the ISO/IEC 27001:2013 (BSI 2013). Annex A is a reference point to determine whether any security measures are absent in an ISMS implementation, but it is not a requirement that organisations select controls from it.

Writing a SOA is not a once-off exercise. The SOA must continually be reviewed and updated. This needs to be done if there are any changes to the risk report, the security controls, or the compliance of the security controls. Previous updates must be documented and kept, as this is a means of providing evidence that there is continuous improvement of implemented controls and the compliance and effectiveness thereof.

3.4.4 ISMS Documentation

The main goal of an ISMS is to allow an organisation to manage information security correctly to ensure the protection of an organisation's information. Documentation is an important dimension of an ISMS as it provides clarity to system users and relevant parties about the management processes and activities of the ISMS. It is an important requirement to document an ISMS during implementation. Documenting an ISMS involves describing the organisation's strategy, its objectives, the risk assessment as well as the security measures selected to mitigate the risk. It also involves the management once the ISMS is operational. At least four levels of documentation exist in organisations as shown in Figure 8.

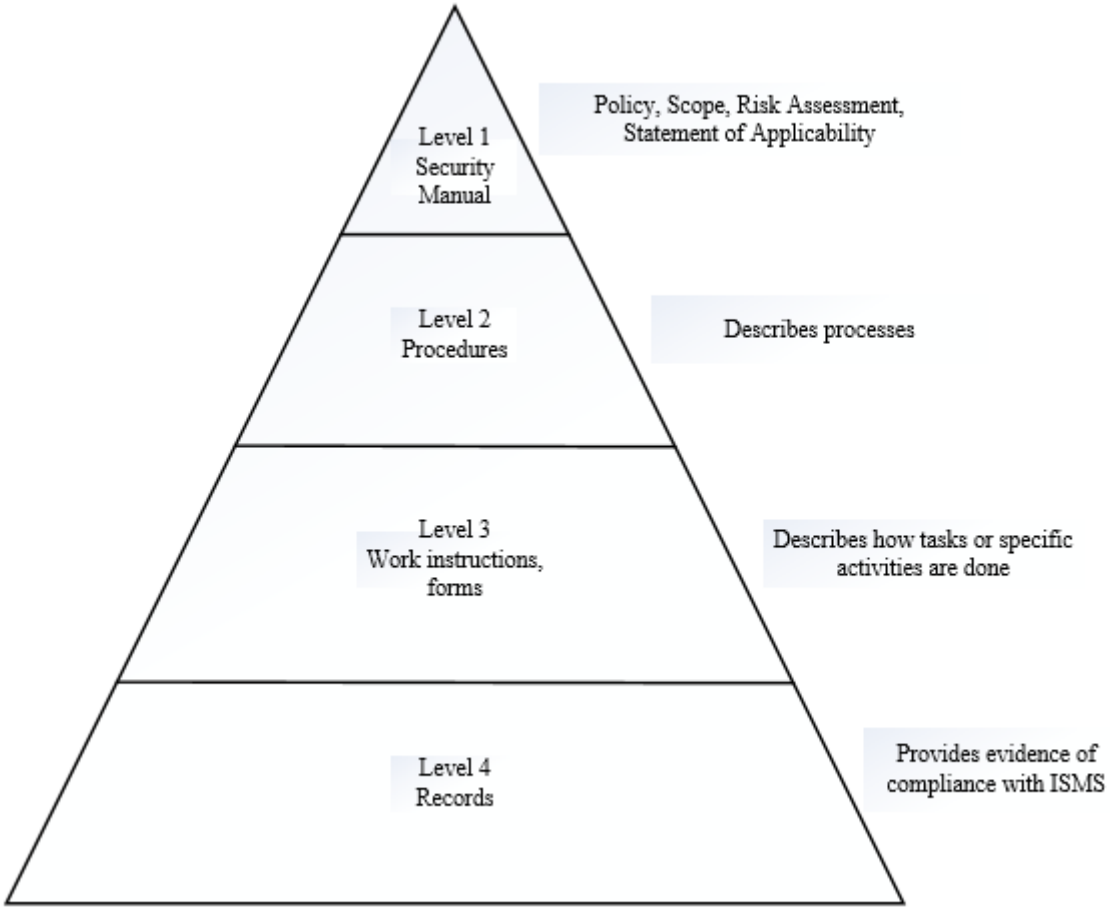

Figure 8: ISMS documentation [Figure 8 in (Saint-Germain 2005)]

ISO/IEC 27001 was designed to provide organisations with the requirements to implement an ISMS, as well for use as a platform for compliance assessments by a certified body to certify an organisation. To comply with ISO/IEC 27001, several mandatory documents and records are required; the organisation needs to develop and provide evidence of these when pursuing certification. Using the latest 2013 version of the ISO/IEC 27001 standard, the documented information and records are listed in clauses four through ten, and include documentation from Annex A of the standard. The required documented information and records (ISO/IEC 27001 2013) are listed in Table 5.

Table 5: ISO/IEC 27001:2013 mandatory documents and records

Clause 4.3	The scope of the ISMS
Clauses 5.2, 6.2	The information security policy and objectives
Clause 6.1.2	The organisations risk assessment and risk treatment methodology
Clause 6.1.3 d	The Statement of Applicability (SOA)
Clauses 6.1.3 e, 6.2	The risk treatment plan
Clause 8.2	The risk assessment report
Clauses A.7.1.2, A.13.2.4	The definition of security roles and responsibilities within the organisation
Clause A.8.1.1	The inventory of assets
Clause A.8.1.3	The acceptable use of assets
Clause A.9.1.1	An access control policy
Clause A.12.1.1	The relevant operating procedures for IT management
Clause A.14.2.5	The organisations secure system engineering principles
Clause A.15.1.1	The supplier security policy
Clause A.16.1.5	The organisations incident management procedure
Clause A.17.1.2	The organisations business continuity procedures
Clause A.18.1.1	Statutory, regulatory, and contractual requirements relevant to the organisation
Clause 7.2	Records of training, skills, and qualifications of the organisations employees
Clause 9.1	The monitoring and measurement results
Clause 9.2	The internal audit program
Clause 9.2	The results of internal audits
Clause 9.3	The results of the management review
Clause 10.1	The results of corrective actions
Clauses A.12.4.1, A.12.4.3	The logs of user activities, exceptions, and security events

Several non-mandatory documents are available, especially in the Annex A section of the standard for organisations to reference for commonly used requirements such as the procedure for document control, procedures for internal audit, mobile device policy, password policy, change management policy, backup policy, information classification policy, and so on. Certification auditors will identify and confirm if the mandatory documented information and records have been developed and are practical for the organisation.

3.5 Overview of ISO/IEC 27002

ISO/IEC 27001 is an auditable standard. The standard mandates specific requirements for the control of information in organisations that claim to have adopted the standard (ISO/IEC 27001 2005). The adoption of the standard means that the organisation is required to adhere to the mandate specified. The requirements as stipulated in the standard are broad, and there is a requirement that organisations that are pursuing registration are required to regularly monitor and review their information security practices. From the research done by Mayer, Haymans and Matulevičius (2006), such requirements are labour intensive as well as a time-consuming exercise. The assumption could therefore, be made that this may be a reason why organisations do not adopt or align to the standard.

ISO/IEC 27002 titled "*Information Technology – Security Techniques - Code of practise for Information Security controls*" is an international standard that provides insight into controls than can be used to protect information and technology (ISO/IEC 27002 2005). The ISO/IEC 27002 standard does not address the implementation of the security measures, but provides guidance of control selection, and how to establish good practises to apply the controls in an environment. The ISO/IEC 27002 standard provides a specification, against which an organisation's ISMS can be audited. Certification is carried out by an accredited, registered certification body. Once an organisation's ISMS has been audited, and if it is found to be compliant, the organisation will be registered as a conforming organisation by a registered certification body and a certification will be granted indicating its compliance (ISO/IEC 27002 2005).

The audit, usually known as the "*Initial Visit*" takes place over several agreed upon days. The standard defines the audit as a two-stage audit. The first stage is an audit of the organisation's documented procedures and processes against the standard to confirm that the organisation complies with the standard. The second stage of the audit is assessing compliance by the organisation with its scope and ISMS. The audit follows a pre-agreed plan where the auditors discuss with the organisation who, when, and in which order they wish to interview employees. The audit uses a negative reporting approach to assess an organisation's ISMS where the organisation is marked down on inadequacies. Non-conformances are categorised as major and minor (ISO/IEC 27002 2005). Major non-conformities indicate that the organisation is not fit for certification at that stage, and the auditor will suggest that the audit

be postponed until the major non-conformities have been resolved. Minor non-conformities indicate improvement opportunities for the organisation.

Based on the results of both stages of the audit, the decision whether the organisation conforms to the standard is made by a review manager who is not part of the assigned audit team. At completion of the audit, the outcome of the audit includes the following (Calder 2009):

- a final written audit report;
- the details of all non-conformities and observations made during the audit;
- an agreed timeline for corrective actions to resolve non-conformities and observations.

As part of the organisation's continuous improvement activities, all observations should be addressed in the post-audit stage to ensure that observations do not turn into non-conformities. If any minor non-conformities were identified in the audit, the certificate will be dependent on resolution of the non-conformities within the agreed timeline. The organisation will then be registered for the standard. The ISO/IEC 27001 registration is valid for three years, but includes an annual reassessment of the ISMS system. Once the certificate has been received, the organisation should display the certificate and start preparing for the first surveillance visit. After three years, a new and complete audit of the ISMS system is necessary for registration.

Organisations can benefit at several levels when competing ISO/IEC 27001 registration as this can be used as assurance of the organisation's capability to manage information security (Saint-Germain 2005). Registration demonstrates that the organisation has implemented suitable security controls, as well as the assurance to ensure that their ISMS and security policies and standards continue to evolve to adjust to the organisation's changing risk factors.

Registration of the standard sets the organisation apart from its competitors, and provides a level of confidence to its clients and vendors. Figure 9, presents the global distribution of ISO/IEC 27001 certificates in 2012.

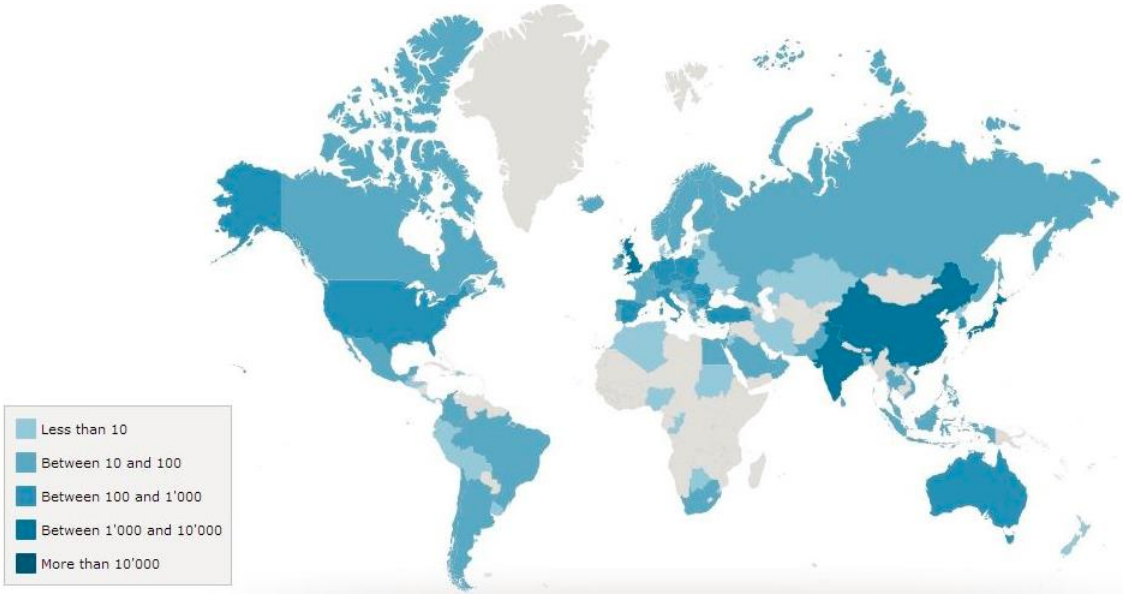

Figure 9: Global distribution of ISO/IEC 2700 in 2012 [Figure 9 from (ISO 2012)]

3.6 Benefits of ISO/IEC 27001

With a picture of the evolution of the standard, and a view of how organisations can utilise it, it is useful to look at the perceived benefits the standard can provide to organisations, as well as the ontological discussions that form part of it. Although many discussions relate to the human-behavioural factors as well as the risk awareness related to experience and knowledge (Parkin et al. 2009), organisations can gain from a number of direct benefits of the implementation of an ISMS and the registration thereof.

A review of the literature relating to the ISO/IEC 27001 standard identifies four main business benefits: (i) compliance, (ii) a marketing advantage, (iii) reduction of long-term costs, (iv) and business control, that an organisation may gain from the implementation thereof (ISO/IEC 27001 2005). The core advantage is that it provides the organisation with a security framework that can be used to mitigate risks associated with information.

As per the benefits discussed in the ISO/IEC 27001 Information Security Research Report Summary (BSI 2012), 87% of the respondents of the survey stated that the implementation of the standard provided a positive outcome to the organisation. Registration of the standard provided organisations with the ability to meet compliance requirements, as well as assist in decreasing the number of raised security incidents. Organisations experienced a growth in external customer satisfaction, with an associated increase in the return of investment and sales despite the increase in IT development and support costs.

The ISO/IEC 27001 standard ensures the protection of information assets within an organisation, but requires an organisation to develop a culture to realise the value of information and the importance to protect and secure it. This can be accomplished through:

- board and senior commitment, accountability and responsibility to information security within the organisation;
- ensuring the correct placement of information security within the organisation structure;
- collaboration between business and IT management regarding information security management;
- effective information security risk management;
- appropriate planning, scoping and security control selection for the initiation and operation of an ISMS within the organisation;
- enforcement of information security compliance, measuring and monitoring; and
- an effective information security education and awareness strategy.

3.7 Challenges of ISO/IEC 27001

Apart from the benefits that the standard provides, it also has some challenges. Von Solms and Von Solms (2004) discuss various aspects that causes difficulties when implementing information security within an organisation. Some of these problems relate to organisations that do not realise that information security is a business responsibility and a requirement for corporate governance and that a well-defined information security governance structure is key to successful ISMS implementation.

A review of the literature relating to the ISO/IEC 27001 standard revealed that there are six challenges that an organisation could face in a successful implementation of the standard, and which could prevent the registration thereof. This may also provide some insight as to why there is limited adoption of the standard by organisations as the perceived challenges may outweigh the apparent benefits. These challenges are identified as (i) obtaining information and support; (ii) translating the technical jargon of ISO 27001 into practical instruction; (iii) integrating ISO 27001 with existing standards and control procedures; (iv) making ISO 27001 "*workable*" in a small business; (v) understanding the ISO audit process; and (vi) selling the perceived benefits to clients (ISO/IEC 27001 2005).

Organisations need to understand and realise the essential components when implementing an ISMS; if they do not, this will ultimately lead to serious flaws in the entire process.

3.8 Summary

This chapter included an overview of the ISO/IEC 27001 standard and the auditing and registration process. The final section explored the alleged benefits that the standard provides to organisations, as well as challenges related to it.

The ISO/IEC 27001 standard provides organisations with a best practice management framework to work with, in the implementation, operation and ongoing maintenance of information security. It provides organisations with the option of complying with the standard or certification thereof. Organisations need to be aware though, that compliance with or certification of the ISO/IEC 27001 standard does not ensure the security of information assets, it only means that the organisation is able to manage information security at the security level which the organisation believes is appropriate and in line with the standard. If there is a flaw at a corporate governance level and in the support from senior management towards the protection of information assets, through to risk assessment regarding the management of information security or how information risk is assessed and managed within an organisation, then it is possible that the organisation may be compliant with the standard, but not secured.

Chapter 4: Research Methodology

This research aimed to investigate the knowledge and understanding of the ISO/IEC 27001 standard within South African organisations. It also investigated who had adopted the ISO/IEC 27001 standard across various sized organisations and industries. Further, we investigated the business objective(s) in adopting ISO/IEC 27001. The research aimed to provide an understanding of the benefits and value an organisation derives from adopting and registering the standard as well as to compare the theory with the actual practice used by organisations in the implementation and registration processes.

This study set out to shed light on the challenges organisations face in the implementation and registration process, which could possibly lead to the abandonment of the project or the decision not to adopt the standard. To test this statement, web-based questionnaires and in-person interviews were conducted to understand current practice.

This chapter discusses the selected research design used in this study.It explains the use of the research design in the methodology section consisting of research instruments, data, and analysis. Also included is a discussion of the limitations of the selected research method. The ethical procedure section details the steps taken to ensure this study adhered to Rhodes University's ethical guidelines.

4.1 Research Design

A survey-based research design was selected for this study. The survey research design consists of gathering data from a sample of entities through their responses to defined questions (Check & Schutt 2012). Survey research designs can collect data relatively quickly without high costs and provide the means of enhancing the understanding of a subject.
Of the various data collection methods available, the survey method is one of the methods that provides several advantages, strengths and benefits that can assist researchers when collecting data (Check & Schutt 2012). The survey-based research method provides the capability of representing a sample frame of a subject. Owing to the number of subject entities who respond to surveys, the data gathered using this method create an overview of the communality of the entities.

Depending on the survey type, administering surveys can generally be a low cost exercise, as the only expenses incurred are the production of the survey questionnaires (Sincero 2014).

Surveys can be distributed in several ways including using the national postal system, or by email or fax. With the vast usage of the Internet, web-based questionnaire surveys have become the preferred way of executing surveys as this is a convenient way of gathering data (Fricker & Schonlau 2002). Because of the varied sample sizes that can be used to conduct a survey, the survey-based method provides an easier approach compared with other data collection methods to collect, analyse and extract statistical significant data.

Although the survey method provides these advantages, it also comes with several disadvantages (Sincero 2014). Surveys provide preciseness, but to accomplish this surveys cannot be changed or restructured once they have been finalised and published, making them an inflexible method once activated. Moreover, survey questions that could result in disagreements or disputes due to misinterpretation or understanding from the participants may result in questions not being answered accurately.

For a survey-based research method to be successful, factors such as the survey design, sampling and measurement of the feedback must be managed thoughtfully (Check & Schutt 2012). If such factors are not taken into consideration when developing the research design, it could lead to possible problems in later stages. Surveys need to be designed to mitigate the risk of sampling, non-coverage, and non-response errors, as well as error of observation and non-observation (Sills & Song 2002; Check & Schutt 2012). Sampling errors occur when a subset of entities are used to represent a subject, resulting in not truly reflecting the overall subject. Non-coverage errors occur if the sample frame does not cover all the required entities of a subject, which could lead to an unbalanced result. Non-response is the difference between the overall entities of a subject that forms part of a survey, and the entities that responded to it. Error of observation is the lack of quality measurement of subjects that are surveyed, which is sourced from elements such as the way questions are designed, written and presented. Errors of non-observation stem from a poor sampling frame resulting in inadequate coverage of a survey and sampling error.

The survey research design was selected for this study because it is an effective method to collect data from a broad-spectrum of sources. The survey consisted of web-based questionnaires, and in-person interviews to collect the required data for this study.

4.1.1 Web-based Questionnaire

A web-based questionnaire is an instrument that is directed to an entity for response. The questions formulated in web-based questionnaires can range from open-ended to close-ended questions used to explore the responses from the entities (Check & Schutt 2012). Although the web-based questionnaire approach is a low cost method for collecting data (Check & Schutt 2012), it still requires a budget to produce as well as re-produce. Web-based questionnaires allow respondents to visit a website where the survey is hosted, and answer the questions in their own time and pace, which normally results in an increase in the response rate. Web-based surveys also provide the means of storing responses automatically in a database that allows the researcher to handle and analyse the data easier as well as limiting the possibility of data errors. Unlike interviews, web-based questionnaires are a lot less time-consuming as well as requiring limited traveling by the researcher.

Closed questions limit the response options of the respondent and provide a quantitative result (Check & Schutt 2012). Unlike interviews, open-ended questions that have no predefined options and require the respondents to answer in their own words, are not as well tolerated in web-based questionnaires, as there is no interviewer to expand or explore the respondents' answers. It is preferable to limit or avoid using open-ended questions, and rather stick to simple and easily understood closed questions for an increase in response rate (Check & Schutt 2012). Web-based questionnaires require a form of computer literacy a well as access to the Internet. Without this, response to the questionnaires would be limited to none. Respondents need to be willing to participate in web-based surveys for the objective of contributing to the research. By participating in surveys to receive some form of incentive may cause inaccurate data.

Web-based questionnaires that are custom built or programmed via online services cannot easily record audio (Thissen 2013). Web-based questionnaires can be built or configured to enable client-side recordings using technology elements such as applets, but the client may not allow this form of access to their system, or it may be blocked by the users' security settings. Web-based questionnaires seldom include voice recordings as responses, and therefore to enrich the data collection techniques, it is essential that interviews with the entities also take place.

4.1.2 Interviews

Compared with web-based questionnaire, the interview approach is a much more personal and exploratory instrument used to collect data. It allows the researcher to explain and expand on the questions asked as well as providing the capability to ask follow-up questions to expand and explore the reasons for a respondent's answer. An interview consists of an interviewer, typically the researcher, and an interviewee, that is, the respondent (Duck & McMahan 2012). Interviews can be used in several survey methods including in-person, telephone, and online interviews (Check & Schutt 2012). The fact that an in-person interview allows the researcher to have direct contact with the respondent to observe and analyse the responses, results in a higher response rate than web-based questionnaires.

Unlike web-based questionnaires, open-ended questions can be more easily tolerated in in-person interviews, as the respondent would be more open to responding with longer answers, as they would have been with written answers. Open-ended questions allow the researcher to analyse the meaning of the respondents' responses, and are ideal for qualitative results (Check & Schutt 2012). Interviews do come with a cost though. It is a time-consuming exercise as the interview will depend on the respondents' availability, traveling that may be required, and scheduling or rescheduling of follow-up sessions as needed (Sincero 2014).

Combining multiple survey types allows the strength of one survey type to compensate for the weakness of the other. Therefore, by using both techniques, web-based questionnaires and in-person interviews for this study, a mixture of qualitative and quantitative data can be obtained, thereby maximising the validity of the data collected from different respondents.

4.2 Research Methods

The technology acceptance model (TAM) is a technology acceptance model used to explain and predict information technology behaviour by users as originally proposed by Davis (1986). TAM provides a model to trace various variables, attitudes, and beliefs as well as intentions in using a technology. As per the model, the use of technology is influenced by the intentions, user's attitude, perceived usefulness, and ease of using the technology.

The research goal of this study was to investigate the adoption of the ISO/IEC 27001 standard in South African organisations. A survey-based research design based on TAM was selected as the data collection method for this study. The research instruments that were used

in this study included a web-based questionnaire and in-person interviews with the sample participants. This methodology was used to collect and analyse data:

- To determine what knowledge South African organisations have of the ISO/IEC 27001 standard;
- To determine who is adopting the ISO/IEC 27001 standard in South Africa;
- To determine the business objective(s) to adopt the ISO/IEC 27001 standard;
- To evaluate the benefits and challenges faced by an organisation in the adoption of the ISO/IEC 27001 standard.

4.2.1 Research Instruments

The research instruments based on the survey-based research design that were used for this study consisted of a web-based questionnaire and in-person interviews. The intention for this data collection method was to have mid to senior level management of an organisation part of the web-based survey as well as the in-person interviews.

Twenty-three participants were identified to participate in the study, each of which received an electronic invitation. The invitation included an introductory statement that explained the motivation of the research as well the actions and information that would be required from the respondent if he/she participated in the survey. Of the 23 identified participants, a total of 18 participants completed the web-based questionnaire, while 15 participants were interviewed in-person.

4.2.1.1 Web-Based Questionnaires

As per Stawarski and Phillips (2008), the following five elements can be included in a questionnaire:

- Open-ended questions – questions that allow the participant to answer in own words;
- Checklists – questions that provide a list of items that the participant can select;
- Two-way questions – questions with limited pairs of responses (for example, Yes or No);
- Ranking scales – questions that allow the participant to rank a list of items;
- Multiple choice questions – questions with several possible answers, from which the participant is required to select one.

For this study, the web-based questions were designed to include checklist and multiple choice questions. This provides a structured questionnaire approach. Open-ended questions were designed and managed in the in-person interviews rather than the web-based questionnaires, as the researcher would be able to expand more on these types of questions with the participant. Two-way and ranking questions were excluded from this study as the selected options were sufficient to achieve the goals of the study. Checklist questions were designed to collect data that could provide an overview of the organisation's use and understanding of the ISO/IEC 27001 standard. Multiple choice questions were used to collect data that could provide an overview of the organisation's structure regarding information security. This heterogeneous structure of questions allowed the researcher to collect descriptive data relevant to the study.

The initial communication with the participants was via a pre-notice email by the researcher. The pre-notice email provided a timed and positive notice to the participant that they would be receiving a formal request to participate in the web-based questionnaire. As per Dillman et al. (2008) it was hoped that sending a pre-notice email for participation in a survey would increase the response rate for the survey. The pre-notice described the reasons for the survey, and what the survey was about.

Two days after the pre-notice email, a formal email was sent to the participants that included an overview of the study, and instructions how to access and complete the web-based questionnaire. The overview contained the title, the description and purpose of the survey, and the name and contact details of the researcher conducting the survey. The instructions section provided the participant with specific instructions on how to access and respond to the questionnaire. The web-based questionnaire was accessible via a link to a commercial website where the survey was hosted. The participants were required to complete the survey within five days of receiving it. Participants were sent reminders before the end-date of the survey to complete any outstanding portions of the survey. Once the survey had been completed, the participant received a thank you email, and availability was discussed with the participants to schedule the in-person interview portion of the study.

The questions for the survey were designed according to the objective of this study. SurveyMonkey[9] is a web-based survey service that was used to conduct the survey as well as to perform basic frequency calculations. The call for participation was directed to the

[9] https://www.surveymonkey.com/

stakeholder who is accountable for information security within the selected organisation. If the accountable stakeholder was not available to complete the web-based questionnaire, the responsible stakeholder of information security or a participant nominated by the accountable stakeholder was approached to complete the questionnaire.

4.2.1.2 In-person Interviews

As part of the survey-based research design, in-person interviews were conducted with the same participants who had completed the web-based questionnaire. The in-person interview was arranged and scheduled after completion of the web-based questionnaire. In-person interviews are an effective data collection method as they allow interaction with the participants and provide the researcher with the ability to delve deeper into responses. Semi-structured interviewing was performed in this study. The questions did not follow any order. Questions were asked as and when additional questions or extension of existing questions were needed for clarification of a subject.

All interviews were pre-arranged. The questions for the in-person interview were designed according to the objective of this study. A pre-notice email was sent by the researcher to the sample participants and stated that the participants would receive a meeting invitation that would consist of an in-person interview. It described the reason for the interview, and what the interview was about. Two days after the pre-notice email, a formal email was sent to the participants that included the meeting request, an overview, and a copy of the questions that would be used during the interview, which the participant could use to prepare themselves for the interview.

The overview section of the email contained the title, the description and purpose of the survey, the structure of the interview, and the name and contact details of the researcher conducting the interview. The interview was conducted with the stakeholder accountable for information security within the organisation. During the interactive interviewing process, the researcher presented the questions verbally, and recorded the structured questions responses as well as spontaneous questions and responses. Each interview lasted between one and two hours.

4.2.2 Reliability and Validity

Straub (1989) identified three elements of instrument validation: content validity, construct validity, and reliability. Content validity requires that the instrument measures be drawn from

all possible measures of the subject being researched. Construct validity requires that measures show stability across methods, while reliability requires that measures show stability across units of observation.

A couple of steps were created to apply instrument validation to this study. A pre-test was established to assess the reliability of the survey. Once the pre-test had been successfully completed, a pilot-test was established and initiated to assess the research validity and reliability.

With the pre-test, qualitative testing commenced on the research instruments. The pre-test was developed to enable revision, which would lead to an instrument that could be validated (Straub 1989).The pre-test was used to test the reliability of the draft web-based questionnaire as well as the in-person interview questionnaire used in this survey-based research to identify vague and unclear questions. The content of the questionnaires was validated by means of expertise from an academic expert in IT to an expert in the topic of this research. The examiners were required to examine the appropriateness, as well as answer, review and evaluate both the web-based questionnaire and the in-person interview questionnaire. Questions that could result in disagreements or disputes due to misinterpretation or understanding by the participants as well as questions whose answers would not contribute to this study were examined. Both the web-based and in-person interview questionnaires were modified to reflect the improvements required to mitigate errors and misinterpretations as per the examiners' feedback.

Once the pre-test had been completed, the pilot-test commenced. The pilot-test was used to further validate the instruments used in this study. The pilot-test targeted a small number of information security specialists. The participants answered both questionnaires and provided feedback to the researcher. The completed questionnaires were reviewed and questions that could result in disagreements or disputes due to misinterpretation or understanding from the participants were modified.

4.2.3 Data

Convenient sampling was selected for this study. Convenient sampling is a non-probability sampling method whereby the researcher selects the subject required for the research by ease of accessibility (Kelley et al. 2003). In any research, it would be ideal to include the entire population of a topic, but in most cases, this is impossible to accomplish. A disadvantage of using the convenient sampling approach is that is does not represent the entire population of a

study, which may lead to potential research problems, as it does not represent the general viewpoint of the entire population.

The objective of this study was to investigate the adoption of ISO/IEC 27001 in South Africa. The 2012 ISO Survey (ISO 2012), which shows the global distribution of ISO/IEC 27001 certificates, indicated that there were 22 organisations that had adopted the ISO/IEC 27001 standard in South Africa. The SABS published the details of eight of the 22 organisations (SABS 2014a). Apart from this publically available information, there is limited information available on organisations that are in the process of adopting the ISO/IEC 27001 standard, have aligned to the standard, or decided not to adopt or align to the standard at all. There is also limited information available about organisations that have adopted the ISO/IEC 27001 standard, but have failed the audit to register their ISMS. As information such as this could damage an organisation's image or credibility to safeguard information (BSI 2012), it is understandable that such companies have not presented themselves publically or made themselves available for participating in this study.

With this in mind, it was clear from the outset that data collection would be difficult and limited. The eight SABS published organisations (as discussed above), as well as organisations that through word of mouth were in the process of adopting the standard were contacted and a request was sent for participation in this study.

4.2.4 Analysis

This section covers the tasks that were executed to analyse the collected survey data as well as preparing, cleaning, and finalising the data for analysis.

Upon completion of the survey data collection, the data were prepared for cleaning. A Microsoft Excel file was created containing all the collected data from both the web-based and in-person questionnaires. The Excel file contained two sheets, one for each questionnaire in order to clean the input appropriately.

Upon completion of preparing the data, the data were cleaned before analysis. This process included checking combinations of variables as well as detecting and handling missing data. Data for adoption of ISO/IEC 27001, organisation size, and industry, were checked first, prior to checking the data for other variables. These variables form part of the core requirements for this survey, and are needed to analyse the survey data by adoption-size-industry. They were used to assist in cleaning the remaining variables. All the collected data

were selected for use, and checked for missing data. Missing data were explored further so that the data analysis was completed in full with attention to these missing data. Missing data were handled differently depending on how many data were missing and the weight of the missing data in the survey. If data that formed part of the core requirements for the survey were missing, then the participant record was excluded from analysis. If data that formed part of the supporting requirements for the survey were missing, then the participant's responses were reviewed to try and recover the missing data.

Once data preparation and cleaning had been completed, the responses from both the web-based and in-person questionnaires were scored according to the ISO/IEC 27001 standard recommendations. Each response was scored and the average response was calculated per section. The average response per section was then calculated to score the response per candidate for the survey. High scoring responses indicated that the participant was aligned to the ISO/IEC 27001 recommendations, whereas low scoring responses indicated that the participant did not align to the ISO/IEC 27001 recommendations. Scoring was done as follows:

Score	Description of Code
5	Strongly agree
4	Agree
3	Neutral
2	Disagree
1	Strongly Disagree

This scoring was useful in comparing participants when analysing the responses. It also provided the ability to compare responses between categories consisting of several groups of questions. The following categories were created to analyse the responses for the various groups:

Category 1	Adoption of ISO/IEC 27001
Category 2	Organisation size
Category 3	Organisation industry

4.3 Limitations of the Method

The major limitation of the selected method for this study is the small sample of organisations that were identified and agreed to participate in this study. It would have been preferable to use all of the 22 ISO/IEC 27001 South African registered organisations (as

mentioned above) for this study. It would also have been ideal if a central, publically available data store was available listing organisations that had adopted but had not registered the ISMS, organisations assessing whether to adopt the standard, organisations that had aligned to the standards, and organisations that had decided not to adopt or align to the standard. Such a data store would have greatly assisted in enhancing the reliability of the findings as well as being able to enrich the generalisation of the results.

Only two publically available web sites provided information related to South African organisations regarding ISO/IEC 27001 adoption (ISO 2012; SABS 2014a). Other than these, only certification bodies and auditing companies that provide assessment services would be able to provide such detail. This form of information is sensitive to an organisation, and could not be shared by the certification bodies and auditing companies for the purpose of this research.

The research method is relevant as the organisations that participated in the study covered all three categories. The research model was designed to be very detailed and was able to collect relevant and valid data. The organisations were able to provide sufficient and detailed feedback when participating in the study.

4.4 Ethical Considerations

All the participants in this study are by definition adults. The participants are professionally qualified and legally competent to take responsibility for their decisions. All the potential respondents to this study received an electronic invitation to participate in the survey. The invitation included an introductory statement that explained the motivation of the research as well as the actions and information that would be required from the respondent if he/she participated in the survey. This provided the respondent the opportunity to accept or decline to participate in the survey.

All the respondents participated freely and on a voluntary basis and were not offered any form of incentive to participate in this study. Their consent to participate in this study was obtained by them once they accepted the electronic invitation sent to them.

For this survey, it will be impossible to provide anonymity as in-person interviews were conducted. For the in-person interviews, the researcher knew the names and addresses of the respondents. The core of this research required that participants provide sensitive organisational information to answers from the survey that should not be publically disclosed.

To prevent any disclosure, subject confidentiality was preserved. Only the researcher had access to the data collected linking each respondent to his/her responses. Access to the collected data was restricted and limited to what was required for this study. Respondents were allocated a sequenced number. Only the provided numbers were used as identification of respondents when required. The information linking a respondent to the provided number was stored in a secure and restricted computer based folder. For additional security, the folder was encrypted using GNU Privacy Guard[10].

SurveyMonkey[11] is a web-based survey service that was used to host and distribute the web-based questionnaire for this study. SurveyMonkey provides security and privacy controls that assured safe and secure online usage of the web-based questionnaire as per the SurveyMonkey Security Statement. All the participants in this study were permitted to voluntary withdraw at any stage of the survey if they wished to do so.

Ethical considerations for this study were influenced by the ethical procedures for the research conducted in the Faculty of Science, at Rhodes University. Ethical clearance for this research, Case No. CS14-04, was granted by the Ethical Clearance Committee of Rhodes University prior to starting the data collection.

4.5 Summary

In this chapter, we discussed the research design used to address the research question of why have so few organisations adopted of the ISO/IEC 27001 standard in South African organisations. We discussed the methodology including the research instruments, data, and analysis, as well as the limitations of the selected research method. The chapter ended with the ethical procedure ensuring this study adhered to Rhodes University's ethical guidelines.

[10] https://www.gnupg.org/
[11] https://www.surveymonkey.com/

Chapter 5: Survey Findings and Analysis

In this chapter, we present an overview of the survey, the research findings, and analysis of the data. The main aim of this work was to investigate the adoption of ISO/IEC 27001 in South Africa. To test this statement, a web-based questionnaire as well as several semi-structured in-person interviews were conducted to understand current practice. The in-person interview findings were used to support the web-based questionnaire findings. The anticipated result of this research is to provide a clearer picture about the adoption of ISO/IEC 27001 by the sample of South African organisations used in this study.

5.1 Overview of the Survey and its Analysis

The web-based questionnaire consisted of the following sections each of which is discussed in the subsequent subsections: demographics, perceived usefulness of the ISO/IEC 27001 standard, attitude towards the use of the standard, social norms, performance expectancy, information security governance, information security risk management, organisation view of the standard, and adoption of the standard. The complete survey is attached as Appendix A.

The survey was designed with these subsections to provide supporting data for the objectives of this study. The demographics subsection provides information about the participants, as well as the industry and size of their organisations. The perceived usefulness of the ISO/IEC 27001 standard subsection provides an overview of the participant's view of the usefulness of the standard within his/her organisation. The attitude towards the use of the standard subsection provides an overview of the organisation's attitude towards the use of the ISO/IEC 27001 standard as well as the adoption thereof. The social norms subsection provides an overview of the organisation's social norms towards the ISO/IEC 27001 standard. The performance expectancy subsection provides an overview of the organisation's performance expectance towards the adoption of the ISO/IEC 27001 standard. The information security governance subsection provides an overview of the organisation's information security governance structure. The information security risk subsection provides an overview of the organisation's information security risk management approach. The organisation view of the standard subjection provides an overview of the organisation's perspective of the standard. The adoption of the standard subjection provides an overview of the adoption of the ISO/IEC 27001 standard within organisations.

Analysis of this research was categorised in three sections. Each category consists of several groups, and the groups are analysed against each other in each category. Using this approach assists in establishing different viewpoints and thus, interpreting the research findings. The following categories with their relevant groups were defined:

- Category 1: Adoption of ISO/IEC 27001
    - Organisations that have adopted ISO/IEC 27001
    - Organisations that have aligned to ISO/IEC 27001
    - Organisations that have not adopted or aligned to ISO/IEC 27001
- Category 2: Organisation size
    - Small organisation: fewer than 50 employees
    - Medium organisation: 50 to 200 employees
    - Medium to large organisation: 200 to 2000 employees
    - Large organisation: more than 2000 employees
- Category 3: Industry
    - Technology and Data Services
    - Marketing and Research
    - Government
    - Retail
    - Financials
    - Automotive
    - Health Care
    - Professional Membership

5.2 Demographic Data

The survey was conducted with stakeholders who are accountable or responsible for information security within their organisation. Table 6 provides a basic breakdown of the 18 participants who participated in the survey, including the participant number, principal industry of the participant's organisation, size of the organisation, and category of adoption.

Table 6: Demographic breakdown

Participant number	Industry	Organisation size	Category of adoption
1	Government	More than 2000 employees	Aligned to ISO/IEC 27001
2	Technology and data services	More than 2000 employees	Aligned to ISO/IEC 27001
3	Automotive	More than 2000 employees	Aligned to ISO/IEC 27001
4	Financials	200 to 2000 employees	Aligned to ISO/IEC 27001
5	Financials	More than 2000 employees	Aligned to ISO/IEC 27001
6	Health Care	More than 2000 employees	Aligned to ISO/IEC 27001
7	Technology and data services	Fewer than 50 employees	Not Adopted ISO/IEC 27001
8	Marketing and research	200 to 2000 employees	Adopted ISO/IEC 27001
9	Technology and data services	Fewer than 50 employees	Adopted ISO/IEC 27001
10	Retail	More than 2000 employees	Aligned to ISO/IEC 27001
11	Technology and data services	200 to 2000 employees	Adopted ISO/IEC 27001
12	Technology and data services	Fewer than 50 employees	Not Adopted ISO/IEC 27001
13	Financials	More than 2000 employees	Aligned to ISO/IEC 27001
14	Professional membership	50 to 200 employees	Not Adopted ISO/IEC 27001
15	Financials	200 to 2000 employees	Not Adopted ISO/IEC 27001
16	Technology and data services	50 to 200 employees	Adopted ISO/IEC 27001
17	Technology and data services	Fewer than 50 employees	Not Adopted ISO/IEC 27001
18	Technology and data services	50 to 200 employees	Aligned to ISO/IEC 27001

Findings showed that 78% of the participants were between the ages of 31 to 45 years and, 22% of the participants were above 45 years of age. The level of education of the participants differed greatly: 11% were in possession of only a high school certificate, 17% had completed a diploma, 22% had completed a bachelor's degree, 5.5% had completed an honours degree, 28% had completed a master's degree, 11% had completed a professional certification in information security, and 5.5% of participants were studying for information security qualifications. The participants' organisation sizes ranged from 22% of organisations consisting of 50 or fewer employees, 17% consisting of between 50 and 200 employees, 22% of organisations consisting of between 200 to 2000 employees, and 39% of organisations consisting of more than 2000 employees.

5.3 Findings and Analysis of Perceived Usefulness

This section of the survey was designed to provide a view of the organisation's perceived usefulness of the ISO/IEC 27001 standard. It assessed the organisation's view whether the standard would improve work quality and make job functions easier and faster. It also assessed the organisation's view whether the standard would provide better control over job functionality and enhance the effectiveness thereof, as well as enable the security of job functions.

Analysis of the research findings showed that 70% of the participants responded that the standard would improve work quality and make job functions easier and faster, whereas 26% of the participants had a neutral view on this, and 4% disagreed that the standard would make job functions easier and faster. The findings showed that 86% of the participants felt the standard provided better control over job functionality and enhanced the effectiveness thereof, whereas 14% had a neutral view thereof.

Based on the results, 94% of the participants felt that ISO/IEC 27001 would enable them to do their job more securely, and 6% responded that it would not.

Across the defined categories with their relevant groups, analysis of the research findings showed overall agreement regarding the perceived usefulness of the ISO/IEC 27001 standard within an organisation. All sizes and types of organisations agreed that the ISO/IEC 27001 standard would improve work quality, as well as enhance job functions by making them easier and faster to do. They further agreed that the standard would be able to provide more control and security over job functionality, and enhance the effectiveness thereof.

5.4 Findings and Analysis of Attitude towards Use

This section of the survey was designed to provide a view of the organisation's attitude towards the use of the ISO/IEC 27001 standard and the adoption thereof. It assessed the organisation's view whether the ISO/IEC 27001 adoption would be beneficial for the organisation. It also questioned whether ISO/IEC 27001 adoption would improve the organisation's information security controls, risk management, compliance and information security governance.

Analysis of the research findings showed that 69% of the participants agreed that adoption of the ISO/IEC 27001 standard would be beneficial to the organisation, and that it would improve the organisation's information security controls, risk management, compliance and information security governance. The findings showed that 22% of the participants had a neutral view thereof, and 9% of the participants disagreed that adoption of the standard could be beneficial and felt that it would not improve the organisation's information security controls.

Across the defined categories with their relevant groups, there was overall agreement regarding the attitude towards the use of the ISO/IEC 27001 standard. From the results,

participants agreed that the adoption of the ISO/IEC 27001 standard would be beneficial for organisations. Based on the results, adoption of the standard would provide improvement of an organisation's information security controls, risk management, compliance and information security governance.

5.5 Findings and Analysis of Social Norms

This section of the survey considered the organisation's social norms towards the ISO/IEC 27001 standard. It assessed the organisation's view of elements that need to be in place before establishing an ISMS, as well as what is already in place. It assessed whether ISO/IEC 27001 adoption should be compulsory in South Africa. It questioned who should be responsible for adopting the ISO/IEC 27001standard in the organisation. It also assessed the organisation's interest in adopting the standard.

5.5.1 Research Findings

Figure 10 provides the participants' responses to what should be implemented first when establishing an ISMS in an organisation.

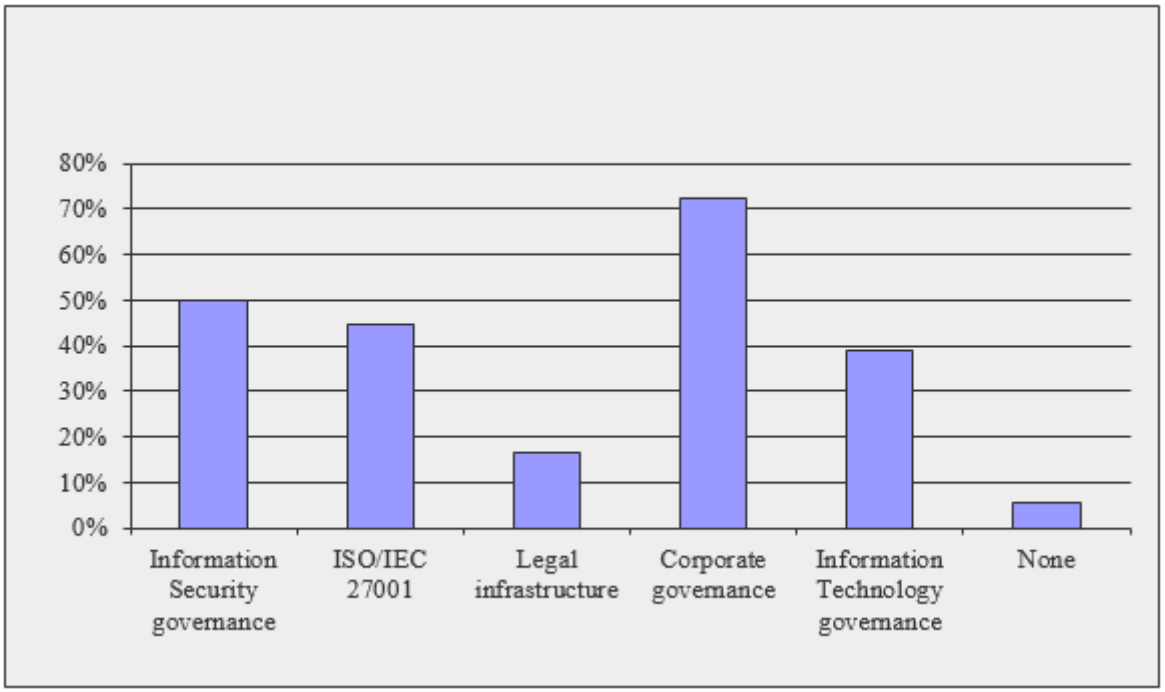

Figure 10: Elements that should be in place before establishing an ISMS

The findings showed that 22% of participants agreed ISO/IEC 27001 adoption should be compulsory in South Africa, 50% of the participants have a neutral view thereof, and 28% of

participants disagreed that ISO/IEC 27001 adoption should be compulsory. If ISO/IEC 27001 adoption became compulsory in our country, 61% of the participants stated that they would do their job considering that both ISO/IEC 27001 was compulsory and it would bring effectiveness to their job, 17% stated they would satisfy all of the requirements of ISO/IEC 27001 on paper since it was compulsory, however their attitude towards doing their job would remain the same as before, 22% stated that ISO/IEC 27001 would not be applied in their organisation even on paper and even if it became compulsory in our country.

Based on the results, 89% of participants' responded that senior management should be responsible for adopting ISO/IEC 27001 as shown in Figure 11.

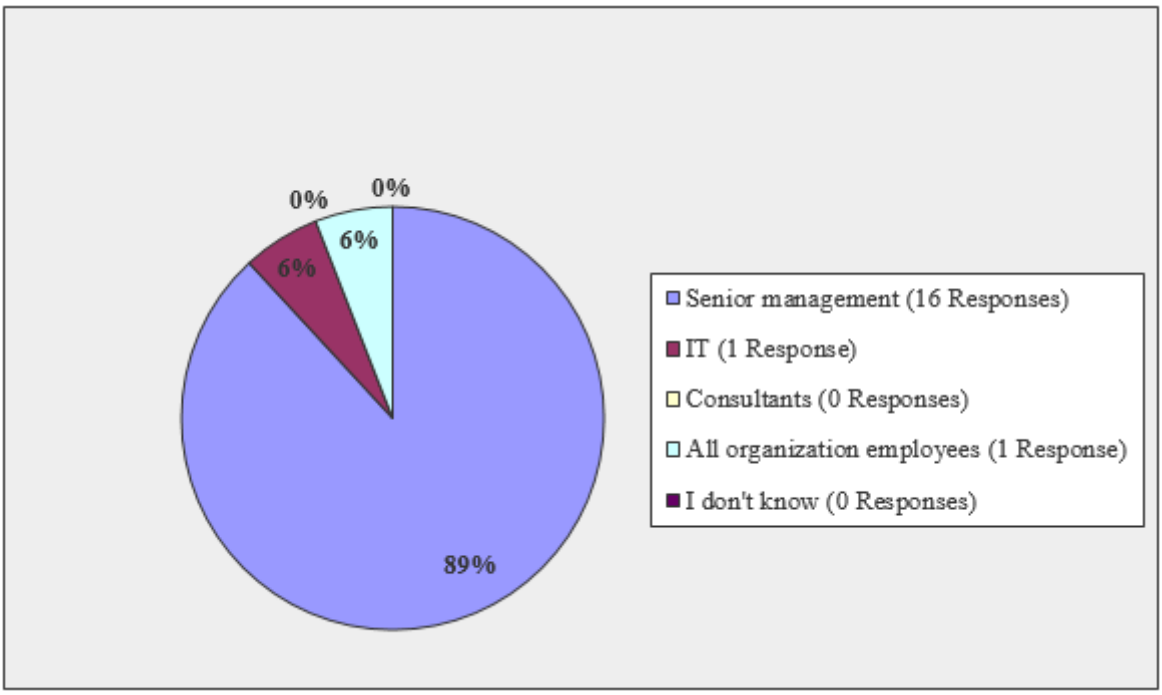

Figure 11: Responsible for adopting ISO/IEC 27001 in an organisation

From the results, 28% of the participants agreed that unless laws were put in place to establish an ISMS, no notice of the adoption of ISO/IEC 27001 would be taken, whereas 22% were neutral and 50% of the participants disagreed with this statement.

5.5.2 Analysis

Adoption of ISO/IEC 27001

Analysis of the research findings showed that organisations that adopted, as well as those aligned to the ISO/IEC 27001 standard, had an understanding of the foundation that is

required for the establishment of an ISMS, and that senior management should be responsible for adopting the standard within an organisation. Analysis of the organisations that adopted and were aligned to the ISO/IEC 27001 standard, showed that there was agreement that ISO/IEC 27001 adoption should be compulsory within South Africa, and that organisations should be taking notice of the international standard.

On the other hand, organisations that had not adopted the ISO/IEC 27001 standard, understood the foundation that is required for the establishment of an ISMS, and agreed that senior management should be responsible for the adoption of the ISO/IEC 27001 within an organisation. The views differed though in that organisations that had not adopted the ISO/IEC 27001 standard disagreed that the standard should be compulsory within South Africa, and adopted the view that unless laws were in place in the country, no action would take place to hasten the adoption of the standard.

Organisation size

The findings showed that small, medium, and large organisations have an understanding of the foundation that is required for the establishment of an ISMS. Medium-to-large organisations had a misunderstanding of the requirements as their view was that corporate governance, IT governance as well as information security governance did not have to be in place in order to establish a successful ISMS. The findings showed that organisations of all sizes understood and agreed that senior management should be responsible for the adoption of the standard within an organisation.

Analysis of the research findings showed that there was little to no agreement that ISO/IEC 27001 adoption should be compulsory in South Africa throughout all sized organisations. If ISO/IEC 27001 adoption was compulsory in our country, small organisations would be the furthest away from compliance than other size companies, as there was limited alignment with the standard. Consensus was that, all sized organisations would only adopt the standard if laws were put in place in the country, otherwise no action would take place to hasten the adoption of the standard.

Industry

Based on the research findings, organisations in the technology and data services, government, financial, automotive, health care, and professional membership industries had

an understanding of the foundation that is required for the establishment of an ISMS. Organisations in the marketing and research as well as retail industries had a misunderstanding as their view was that corporate governance, IT governance as well as information security governance did not have to be in place to establish a successful ISMS. Organisations across the range of industries have the same viewpoint that senior management should be responsible for the adoption of the standard within an organisation. Only organisations in the retail industry agreed that adoption should be compulsory in South Africa. If adoption was compulsory, organisations in the technology and data services industries would be the furthest away from compliance than other industries, as there was low adoption of the standard in this industry. Organisations in the technology and data services, government, financial, and health care industries would only adopt ISO/IEC 27001 if laws were put in place in the country, otherwise no action would take place to hasten the adoption of the standard.

5.6 Findings and Analysis of Performance Expectancy

This section of the survey was designed to provide a view of the organisation's performance expectance towards the adoption of the ISO/IEC 27001 standard. It assessed the organisation's view whether there would be a decrease in performance when adopting ISO/IEC 27001. It also assessed the organisation's view whether job performance and job efficiency could be driven simultaneously with ISO/IEC 27001 in the organisation.

5.6.1 Research Findings

The results concluded that 78% of the participants disagreed that there would be a decrease in performance when adopting ISO/IEC 27001, whereas 22% had a neutral view thereof. The findings showed that 83% agreed that job performance and efficiency could be driven together with ISO/IEC 27001 in the organisation, whereas 17% had a neutral view thereof.

5.6.2 Analysis

Analysis of the research findings showed that organisations that adopted, aligned to, as well as those which have not adopted the ISO/IEC 27001 standard, and organisations of various sizes in different industries, agreed that the organisation's performance expectation towards the adoption of the ISO/IEC 27001 standard would not decrease. Based on the findings, organisations agreed that there would be an enhancement in job performance and efficiency and both could be driven simultaneously with ISO/IEC 27001.

5.7 Findings and Analysis of Information Security Governance

This section of the survey provides a view of the organisation's information security governance structure. It assessed the organisation's compliance with King III, particularly the section related to the ISMS requirement, and the understanding of IT and information security governance. It questioned whether roles and responsibilities for information security as well as a governance structure for information security had been defined in the organisation. It identified whether the organisation had an information security strategy and whether business and technology executives were engaged when developing the strategy. It assessed whether the organisation had an information security policy as well as the frequency of information security reporting to senior management. It also determined the barriers the organisation faced in ensuring information security.

5.7.1 Research Findings

Twenty-eight percent of participants stated that their respective organisation complied with King III, whereas 39% were partially compliant, and 22% were noncompliant. The findings showed that 11% of the participants were not sure if they complied with King III.

Based on the results, 44.5% of the participants responded that their respective organisation had a developed and implemented ISMS as per King III, 44.5% confirmed that no ISMS was in place, and 11% were not sure if an ISMS had been developed and implemented.

The in-person interviews showed that 80% of the organisations had an understanding of what IT governance was about, whereas only 67% of the organisations understood what information security governance was. From the results, 67% of participants responded that a governance structure for information security did exist in the organisation, whereas 33% responded that this was not the case.

The in-person interviews concluded that 87% of the organisations had an understanding of what IT security was, whereas 73% of the organisations understood what information security was.

Seventy-two percent stated that roles and responsibilities for information security in their respective organisations had been defined whereas 28% responded that this was not the case. The findings showed that 78% of the organisations had an executive(s) responsible for information security, whereas 22% did not.

Results from the in-person interviews showed that 87% of the organisations had a direct line of communication or committees in place to inform the organisation's board of directors and shareholders of information security related matters. The findings showed that 13% responded that information security related matters were not communicated to their organisation's board of directors or shareholders.

Based on the results, 50% of the participants responded that the person responsible for information security reported directly to the owner \ Chief Executive Officer (CEO) \ board of directors \ managing director of the organisation, 22% stated that the relevant person reported to the Chief Information Office (CIO) \ senior executive, while 11% reported to the Chief Financial Officer (CFO), 6% reported to legal and compliance, and 11% responded that no reporting to senior management regarding information security took place.

Analysis of the findings showed that 89% of participants responded that senior management who were responsible for information security had several additional functions as part of their scope of work. These functions included information security governance, information security strategy and planning, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, information security compliance, and information security risk assessments. The findings showed that 11% responded that information security functions were not part of senior management's scope of work.

Sixty-one percent of organisations had a documented and approved information security strategy, 5% responded that their organisation had a documented but not approved information security strategy, 17% responded that they intended to get a strategy documented and approved, and 17% responded that there was no strategy in place.

The results concluded that 61% of organisations actively engaged both line of business and technology executives in identifying requirements for the organisation's information security strategy, 17% responded that only one of the lines of executives were engaged, and 22% responded that neither lines of business nor technology executives were engaged, or they were not aware that engagement was taking place.

The findings showed that 61% of participants had a documented and approved information security policy that included a framework for setting objectives, taking into account

contractual, legal and regulatory requirements aligned to the information security risks to the business and established the criteria for risk evaluation. From the results, 6% responded that a documented information security policy was in place but not approved, 11% intended to have one documented and approved, and 22% did not have an information security policy as shown in Figure 12.

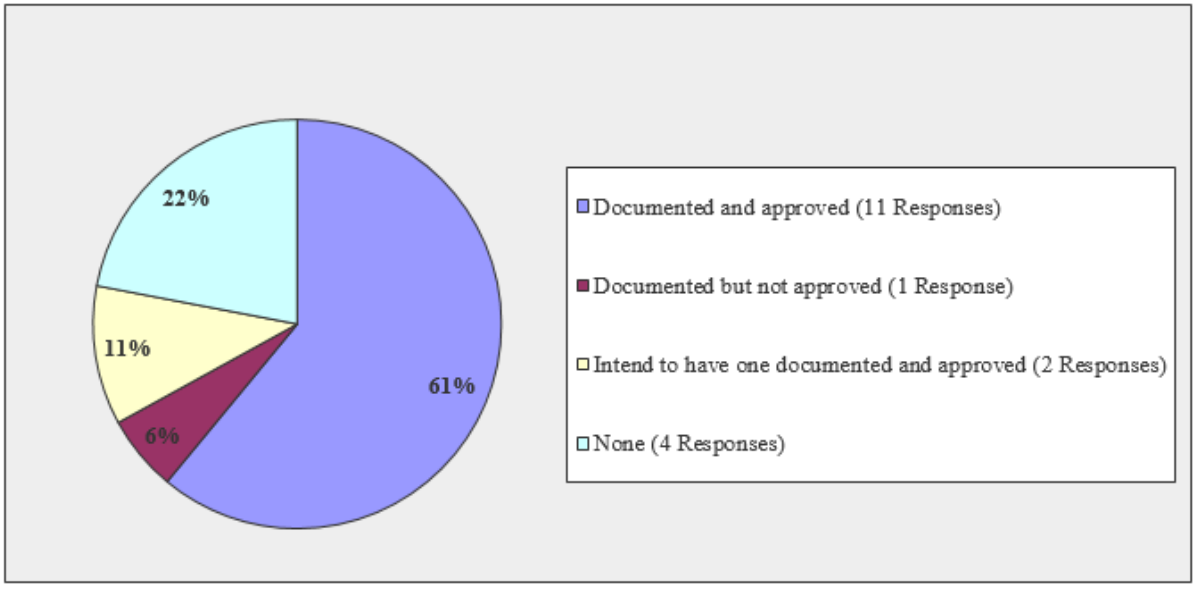

Figure 12: Organisations with an information security policy

Results show that organisations faced major barriers when ensuring information security. These barriers include lack of sufficient budget, lack of support from business lines, lack of information security visibility and influence within the organisation, lack of security knowledge, lack of executive support, and insufficient staff and time to drive and run the management system.

From the findings, 61% of participants responded that monthly / quarterly reports were provided to senior management on information security status and the posture of the organisation, 5.5% responded that information security reporting took place on an ad hoc basis, 28% responded that information security was not reported to senior management, and 5.5% did not know if reporting was done.

5.7.2 Analysis

Adoption of ISO/IEC 27001

Analysis of the research findings shows that there is minimal alignment to King III covering corporate governance by organisations that adopted, were aligned to, or had not adopted the

ISO/IEC 27001 standard. This implies that there is minimal adoption of the King III requirements to ensure that information is adequately protected and that an ISMS is developed and implemented throughout the organisation.

These results indicate that organisations that have adopted, or aligned to the ISO/IEC 27001 standard have a governance structure for information security, an executive responsible for information security, an information security strategy, an information security policy, as well as defined roles and responsibilities for information security within the organisation. Organisations that have not adopted the standard, do not have a governance structure in place, do not have an executive responsible for information security, and do not have defined roles and responsibilities within the organisation for information security. The findings show that 20% of organisations that have not adopted the standard have an information security policy in place. Organisations that have adopted, or aligned to the standard, do monthly and quarterly reporting to senior management regarding information security related matters, where limited reporting is done by organisations that have not adopted the standard.

Analysis of the research findings shows that the executives responsible for information security within organisations that have adopted, and are aligned to the ISO/IEC 27001 standard have several additional functions within their scope of work. These functions include information security governance and compliance, information security strategy and planning, information security risk management, asset security and management, operations security, supplier relationships, and information security aspects of business continuity management. Engagement levels for security matters included business and technology executives.

Organisations that have adopted, are aligned to, or have not adopted the standard are faced with major barriers when ensuring information security within their organisation. These barriers include lack of support from business lines, lack of sufficient budget, lack of information security visibility and influence within the organisation, lack of executive support, and insufficient staff to drive and run an ISMS.

Organisation size

Based on the research findings, there is minimal alignment to King III covering corporate governance by organisations of all sizes. This leads to minimal adoption of the King III requirements to ensure that information is adequately protected and that an ISMS is

developed and implemented. Only medium-to-large, and some (57%) large organisations are aligned with King III regarding the development and implementation of an ISMS.

Analysis of the research findings shows that medium, medium-to-large, and large organisations have a governance structure for information security, an information security strategy, an information security policy, as well as defined roles and responsibilities for information security within the organisation. Analysis shows that 75% of small organisations have no information security governance structure in place, do not have an information security strategy, do not have an information security policy in place, and have not defined roles and responsibilities within the organisation for information security. Organisations of all sizes do have an executive responsible for information security that receives a monthly or quarterly report regarding information security related matters.

The findings show that the executive responsible for information security within the organisation has several additional functions within his/her scope of work. These functions include information security governance and compliance, information security strategy and planning, information security risk management, asset security and management, operations security, supplier relationships, and information security aspects of business continuity management. Engagement levels for security matters includes business and technology executives.

Organisations of all sizes are faced with major barriers when ensuring information security within their organisation. These barriers include lack of support from business lines, lack of sufficient budget, lack of information security visibility and influence within the organisation, lack of executive support, and insufficient staff to drive and run an ISMS.

Industry

Based on the results, there is alignment with King III that covers corporate governance from organisations in the marketing and research, automotive, health care, and professional membership industries. This has led to the adoption of the King III requirements to ensure that information is adequately protected and that an ISMS is developed and implemented accordingly. There is limited-to-no alignment with King III regarding the development and implementation of an ISMS by organisations in the technology and data services, government, retail, and financial industries.

Organisations in the marketing and research, technology and data services, government, financials, automotive, health care, and professional membership industries have a governance structure for information security, an information security strategy, as well as defined roles and responsibilities for information security. Organisations in the retail industry have no information security governance structure in place, do not have an information security strategy, and have not defined roles and responsibilities for information security. Organisations in the retail and automotive industries do not have an approved information security policy in place. Organisations in all the mentioned industries do have an executive responsible for information security and received monthly and quarterly reports regarding information security related matters.

Analysis of the research findings shows that the executive responsible for information security within the organisation has several additional functions within his/her scope of work. These functions include information security governance and compliance, information security strategy and planning, information security risk management, asset security and management, operations security, supplier relationships, and information security aspects of business continuity management. Engagement levels for security matters include business and technology executives.

The major barriers organisations in the various industries face when ensuring information security within the organisation range from lack of support from business lines, lack of sufficient budget, lack of information security visibility and influence within the organisation, lack of executive support, and insufficient staff to drive and run an ISMS.

5.8 Findings and Analysis of Information Security Risk Management

This section of the survey provides a view of the organisation's information security risk management. It assessed whether the organisation has an information security risk methodology, risk treatment plan, and risk register. It also assessed whether the organisation has an information security training and awareness programme.

5.8.1 Research Findings

Analysis of the research findings shows that 56% of participants responded that their organisation had a documented and approved risk methodology, 11% responded that their organisation had a documented methodology, which was not approved. The findings show

that 22% of the participants responded that they intended to get a risk methodology documented, whereas 11% responded that no risk methodology existed.

The in-person interviews showed that 100% of the participants responded that through workgroups or by direct line, senior management as well as business was involved when reporting and rating the severity of identified risks.

Based on the results, 39% of participants responded that the organisation had a documented risk treatment plan that identified actions, resources and funding, as well as responsibilities and priorities for managing information security risks, 17% responded that a documented risk treatment plan existed, but was not approved. The findings showed that 33% of the participants stated that they intended to get a risk treatment plan documented, whereas 11% responded that no risk treatment plan existed.

Findings from the in-person interviews showed that 87% of the participants confirmed that senior management was involved when selecting as well as approving information security risk treatment options, and 47% responded that ISO/IEC 27001 was used as a guideline when selecting treatment options.

Results from the in-person interviews confirmed that 53% of the organisations measured the effectiveness of the security controls implemented to mitigate risks, whereas 47% responded that measurements were not being done formally on mitigating controls.

Fifty percent of participants responded that the respective organisation had an up-to-date risk register that specified information security related risks, 11% responded that the organisation had a risk register that specified information security related risks but which was not updated. The findings show that 11% of the participants responded that there was a risk register but this did not specify information security related risks, 6% responded that a risk register existed but was not updated nor specified information security related risks, whereas 22% responded that no risk register existed as shown in Figure 13.

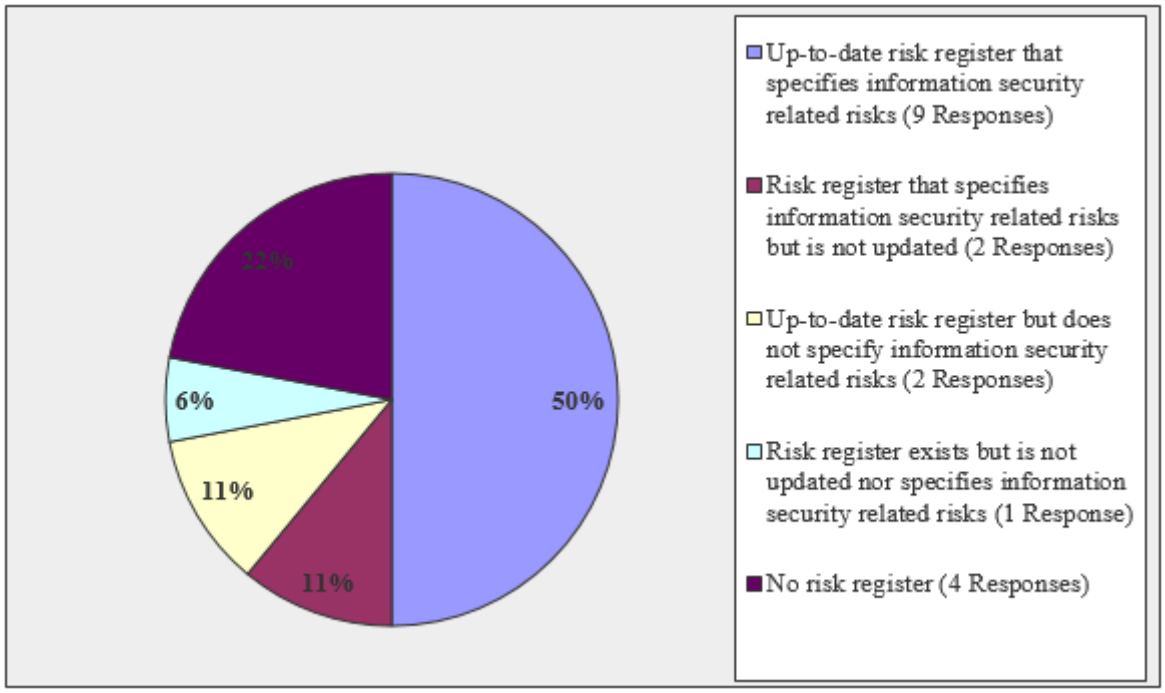

Figure 13: Organisation's risk register

Based on the results, 67% of the participants responded that their risk treatment process was able to define which security controls should be implemented to mitigate an identified risk, 28% responded that their risk treatment process was not able to do so, whereas 5% were uncertain whether the risk treatment process was able to do so.

The findings showed that 39% of the participants responded that their organisation had an information security training and awareness programme documented, approved and implemented, while 5% stated that this still had to be implemented. The findings show that 22% of the participants responded that the program is documented, but not approved or implemented, 17% responded that they intended to have one documented, approved and implemented, whereas 17% responded that such a program did not exist (see Figure 14).

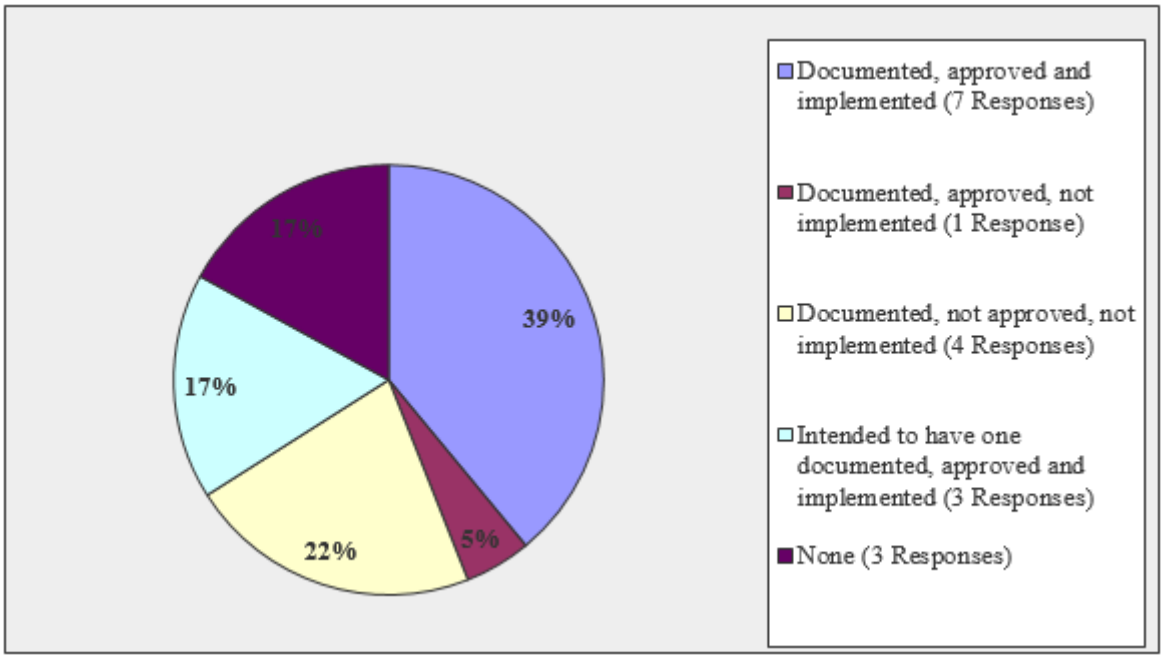

Figure 14: Organisations information security awareness plan

5.8.2 Analysis

Adoption of ISO/IEC 27001

Analysis of the research findings shows that organisations that have adopted, are aligned to, or have not adopted the ISO/IEC 27001 standard, do have a risk methodology in place in the organisation. Organisations that have adopted, or are aligned to the standard have a risk treatment plan, a risk treatment process, which is able to define which security controls should be implemented to mitigate an identified risk, as well as a risk register that specifies information security related risks in place. Organisations that have not adopted the standard, have limited-to-no risk registers or treatment plans in place in the organisation.

An information security training and awareness programme does exist in organisations that have adopted, or are aligned to the standard, whereas such a programme does not exist in organisations that have not adopted the standard.

Organisation size

Based on the results, medium, medium-to-large, and large organisations do have a risk methodology, a risk treatment plan, a risk treatment process, as well as a risk register that specifies information security related risks in place. These larger organisations also have an

information security training and awareness programme in place. Small organisations have limited-to-no risk approach or security awareness program in place.

Industry

The findings show that organisations in the marketing and research, automotive, health care, technology and data services, financial and professional membership industries, do have a risk methodology, a risk treatment process, a risk register that specifies information security related risks, as well as an information security training and awareness programme in place in the organisation. Organisations in the marketing and research, automotive, health care, technology and data services, and professional membership industries do have a risk treatment plan that identifies actions, resources and funding, as well as responsibilities and priorities for managing information security risks in place, whereas organisations in the retail, government, and financial industries are still in the process of developing these.

Organisations in the retail and government industries are behind the rest of the industries, as items such as a risk methodology, a risk treatment process, a risk register, and an information security training and awareness programme are not in place.

5.9 Findings and Analysis of Organisation's View of ISO/IEC 27001

This section of the survey was designed to provide an organisation's view of the ISO/IEC 27001 standard. It questioned the organisation's awareness of ISO/IEC, the ISO/IEC 27001 standards, and other ISO related standards. It identified the perceptions of different organisation sizes and industries with regard to what the ISO/IEC 27001 was designed for.

5.9.1 Research Findings

Analysis of the research findings shows that 83% of the participants responded that their respective organisation was aware of the ISO/IEC, as well as ISO standards such as ISO 9001, ISO 31000 and ISO 14001. The findings show that 17% responded that the organisation was not aware of these, or did not know if the organisation was aware of the standards. Figure 15 shows the management systems in place at each participant's organisation.

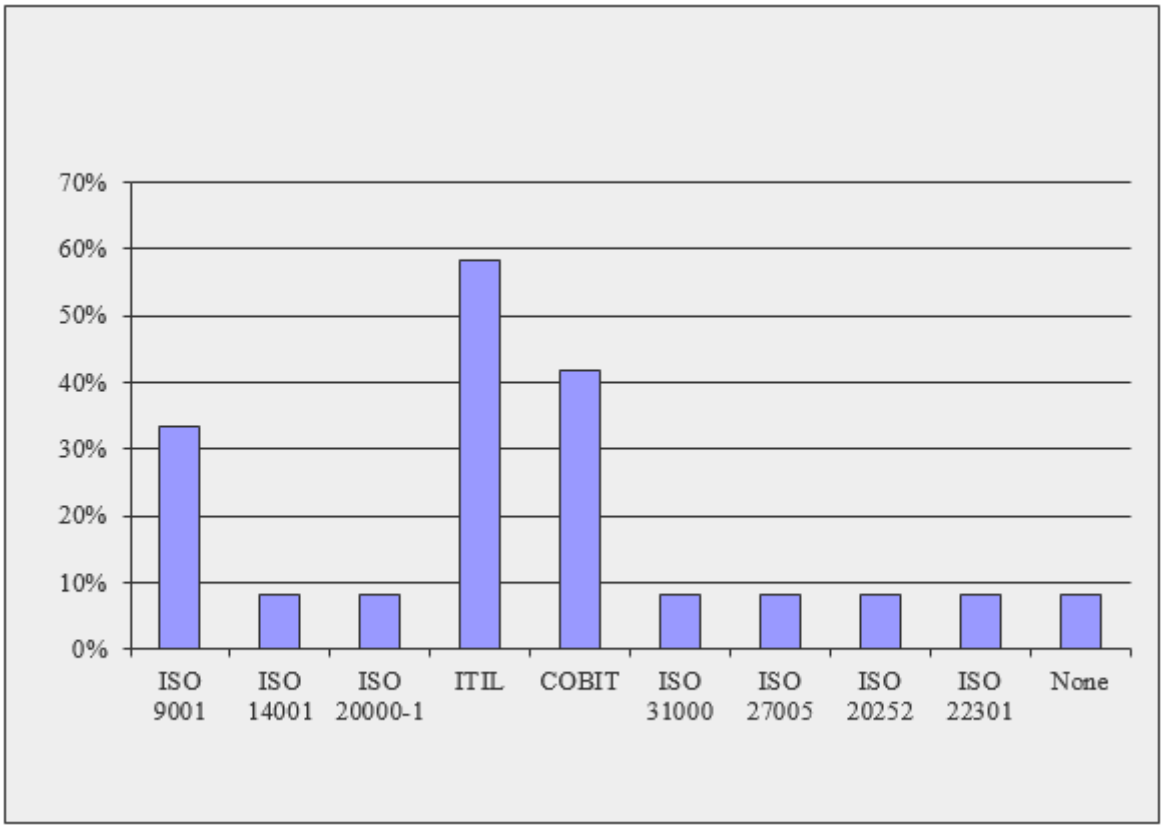

Figure 15: Management systems in place at each organisation

Eighty-three percent of the participants responded that they were aware of the ISO/IEC 27001 standard, whereas 17% were not aware of it. Findings from the in-person interviews showed that 53% of the organisations understood the concept of an ISMS, whereas 47% did not. The in-person interviews showed that 33% stated that their respective organisations did have an understanding of how ISO/IEC 27001 describes the ISMS, and 67% responded that their organisation had limited-to-no knowledge thereof. Results of the in-person interviews showed that 73% of the organisations (owing to the adoption of other management systems) understood the concept of the PDCA model, while 27% did not understand the concept.

Based on the results, 67% of the participants responded that the ISO/IEC 27001 standard had been designed for and was expected to be used by any size organisation. The findings showed that 17% responded that the standard was designed for large organisations with more than 2000 employees, 11% responded that it was designed for medium-to-large sized organisations with fewer than 2000 employees, and 5% responded that they did not know. Figure 16 shows the industries the participants believed the ISO/IEC 27001 standard was designed for and expected to be used by.

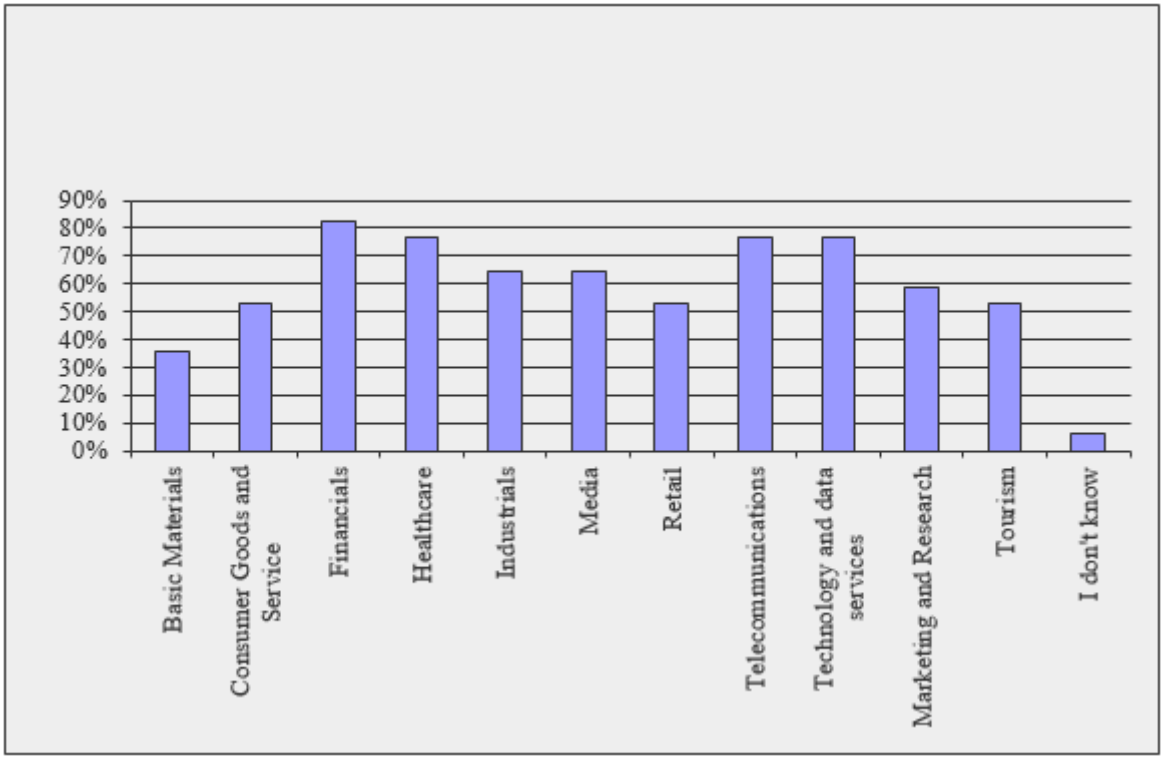

Figure 16: Industries ISO/IEC 27001 has been designed for as per responses

5.9.2 Analysis

Adoption of ISO/IEC 27001

Analysis of the research findings shows that organisations that have adopted, were aligned to, or have not adopted the ISO/IEC 27001 standard are aware of the ISO/IEC and the available standards from this organisation such as ISO 9001, ISO 31000 and ISO 14001. Organisations that have adopted, or were aligned to the ISO/IEC 27001 standard, have implemented other management systems in the organisation including ISO 9001, ISO 14001, ISO 20000-1, ITIL, COBIT, ISO 31000, ISO 27005, ISO 20252, and ISO 22301. The following management systems and standards are being used by organisations:

- Organisations that have adopted ISO/IEC 27001 also implemented: ISO 9001, ISO 20000-1, ITIL, COBIT, ISO 20252, ISO 22301
- Organisations that are aligned to ISO/IEC 27001 also implemented: ISO 9001, ISO 14001, ITIL, COBIT, ISO 31000, ISO 27005
- Organisations that have not adopted ISO/IEC 27001 implemented: ITIL

Based on the results, organisations that have adopted, or are aligned to the ISO/IEC 27001 standard are aware that the ISO/IEC 27001 standard was designed for adoption by any size

organisation. Organisations that have not adopted the standard, indicated that the ISO/IEC 27001 standard was only designed for adoption by medium-to-large and large organisations.

Organisations that have adopted, are aligned to, or have not adopted the ISO/IEC 27001 standard indicated that there is a general awareness that the ISO/IEC 27001 standard has no limitations and is not industry specific, and could be adopted by an organisation in any industry.

Organisation size

The findings show that organisations of all sizes are aware of the ISO/IEC and the available standards from the organisation such as ISO 9001, ISO 31000, ISO 14001 as well as ISO/IEC 27001. Medium, medium-to-large, and large organisations have implemented other management systems including ISO 9001, ISO 14001, ISO 20000-1, ITIL, COBIT, ISO 31000, ISO 27005, ISO 20252, and ISO 22301. Small organisations though, have not implemented any other management systems.

Organisations of all sizes have a general awareness that the ISO/IEC 27001 standard has no limitations and was designed for adoption by any size organisation, and there is a general awareness that the ISO/IEC 27001 standard is not industry specific, and could be adopted by an organisation in any industry.

Industry

Based on the results, apart from government, organisations in the marketing and research, technology and data services, retail, automotive, health care, technology and data services, financial and professional membership industries are aware of the ISO/IEC. Apart from organisations in the financial industry, the rest of the industries that formed part of this study are aware of related ISO standards such as ISO 9001, ISO 31000, ISO 14001.

Apart from ISO/IEC 27001, other management systems implemented per industry are as follows:

- Marketing and research: ISO 9001, ISO 20252
- Technology and data services: ISO 9001, ISO 20000-1, ITIL, COBIT, ISO 22301
- Government: ITIL
- Retail: None

- Financial: ITIL, COBIT, ISO 31000
- Automotive: ISO 9001, ISO 14001
- Health care: ITIL, COBIT, ISO 27005
- Professional membership: ITIL

Analysis of the research findings shows that government and organisations in the professional certification industries indicated that the ISO/IEC 27001 standard was designed for adoption by large organisations. Organisations in the rest of the industries that participated in this study have a general awareness that the standard has no limitations and was designed for any size organisation. Government indicated that the standard was only designed for the telecommunications and technology and data services, while organisations in the health care industry indicated that the standard was only designed for the health care industry. Apart from the government and health care industries, organisations in the rest of the industries that participated in this study have a general awareness that the standard has no limitations and was designed for adoption by any industry.

5.10 Findings and Analysis of ISO/IEC 27001 Adoption

This section of the survey was designed to provide a view of the adoption of the ISO/IEC 27001 standard. It assessed the objective for adopting the standard, senior management support, and whether a business case was developed for the adoption of the standard. It assessed management commitment towards an ISMS. It assessed whether the organisation had an ISMS scope, SOA, or a document control framework that included a review process, and whether the organisation was aware of the mandatory documents and records required by ISO/IEC 27001 for adoption purposes. It assessed the benefits and challenges the organisation faced to adopt ISO/IEC 27001 standard, the implementation timescale, the resources used for implementation, implementation costs, and if the organisation were to implement ISO/IEC 27001 again, what they would do differently.

5.10.1 Research Findings

Based on the results, 22% of the organisations that participated in the survey have adopted the ISO/IEC 27001 standard, 50% are aligned to the standard, and 28% of the organisations have not adopted or aligned to the standard as shown in Figure 17.

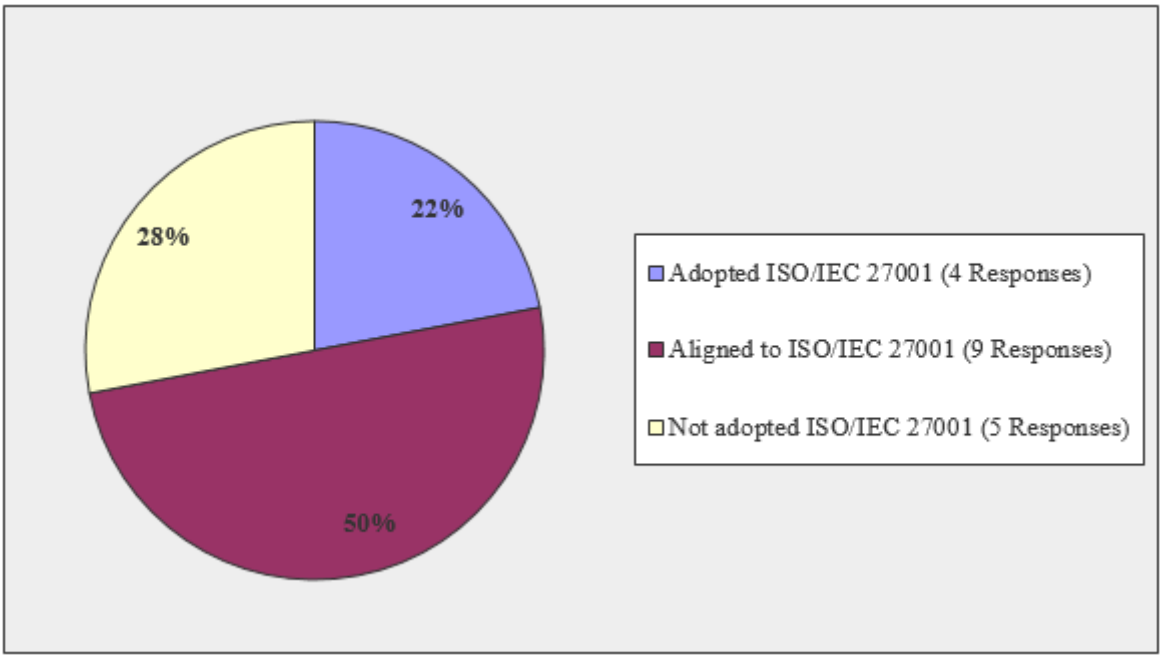

Figure 17: Adoption of ISO/IEC 27001

Seventy-two percent of the participants responded that there was an objective to adopt the ISO/IEC 27001 standard within the organisation. The objectives for adoption included that this had been mandated by a customer or holding company, adoption was a requirement when tendering, adoption would provide a competitive advantage, the standard was recognised as a best practice standard, adoption would ensure legal and regulatory compliance, adoption would establish trust to other parties, and adoption would have provided optimisation in the organisation. The findings show that 28% of organisations have not adopted the standard and have no objective for doing so.

Based on the results, 66% of the participants responded that senior management support was obtained with the decision to adopt or not adopt the standard, 17% responded that there was no senior management support obtained, and 17% responded that they did not know if senior management support was obtained.

The findings show that 28% of the participants responded that a business case was developed and approved when the decision was made to adopt the standard. Based on the findings, 11% responded that they intended to have a business case developed and approved, 44% responded that no business case had been developed, while 17% stated that they did not know if a business case had been developed.

Twenty-eight percent of the participants responded that the business case for the adoption of the standard included the certification of the ISMS, 55% responded that the business case did not include certification, and 17% responded that they did not know if the business case included certification of the ISMS.

Analysis of the research findings shows that 55% of the participants responded that management provided commitment to the ISMS, such as establishing an information security policy and objectives as well as communicating the importance of meeting those objectives with the organisation, 28% responded that management did not provide commitment to the ISMS, and 17% responded that they did not know if management provided support.

The findings show that 44% of the participants responded that their organisation had a documented and approved ISMS scope, 5.5% responded that approval of the scope was still required, 17% responded that the organisation intended to have one documented and approved, 28% responded that an ISMS scope did not exist, and 5.5% responded that they did not know if an ISMS scope existed as shown in Figure 18.

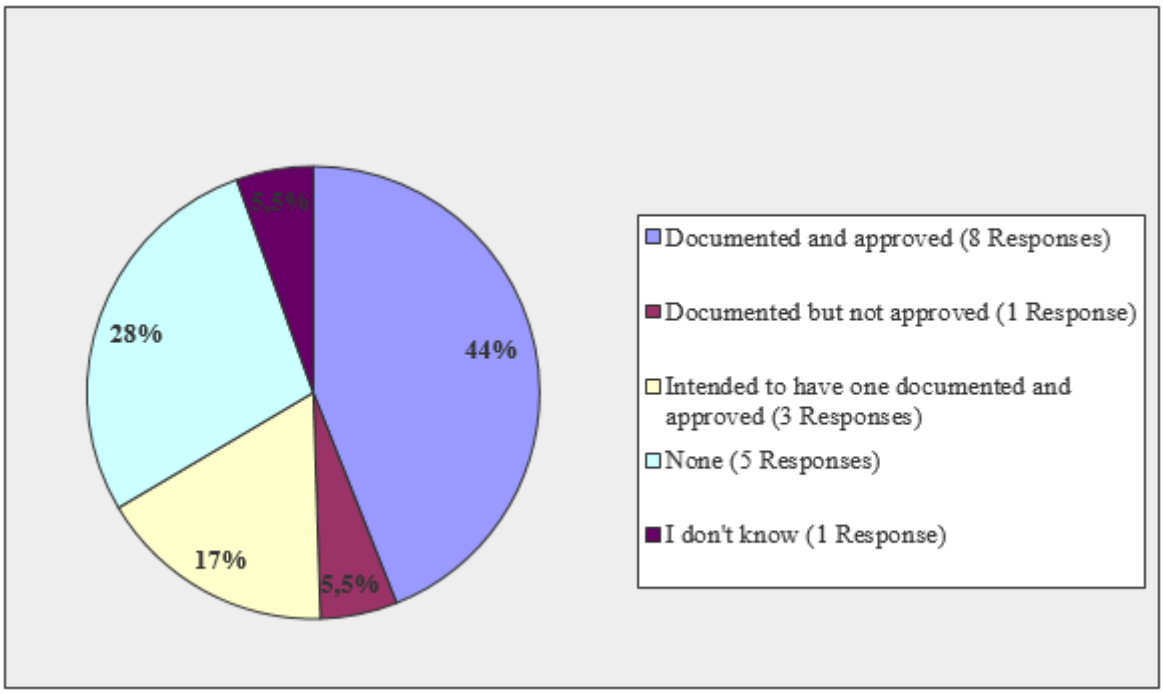

Figure 18: ISMS scope document

The in-person interviews showed that 39% of the participants responded that their organisation had a documented and approved ISMS SOA, 11% responded that the organisation intended to have one documented and approved, 39% responded that an SOA did not exist, and 11% responded that they did not know if an SOA existed.

Results of the in-person interviews show that 28% of the participants responded that the organisation had a documented and approved document control framework in place, 22% responded that approval was still required, and 50% responded that a document control framework did not exist in the organisation.

The findings showed that 50% of the participants responded that the organisation's review process for documentation did occur bi-annual to annually, 22% responded that documents were only reviewed once massive changes occurred in the organisation, and 28% responded that they did not know about the organisation's review process for documentation.

Forty-four percent of the participants responded that the organisation was aware of the mandatory documents and records required when adopting the standard, 39% responded that they were not aware, while 17% responded that they did not know if the organisation was aware of the mandatory documents and records.

A total of 73% of the participants responded that there were several benefits the organisations received from adopting as well as aligning their ISMS with the ISO/IEC 27001 standard. These included a better structure regarding information security within the organisation. Adoption provided the ability to identify and manage information security risks in the organisation, and manage incidents more appropriately. It provided a market edge in the industry and drove business value to the organisation's customers and suppliers, while creating more awareness of information security within the organisation. Adoption of the standard made senior management aware that information needed to be seen as an asset to the organisation and that it needed to be protected. Alignment created an increase in overall information security and implementation of controls that protected the company from financial and reputational damages.

Based on the results, the main barriers organisations faced in ensuring information security were a lack of information security visibility, influence, and support from business lines as shown in Figure 19.

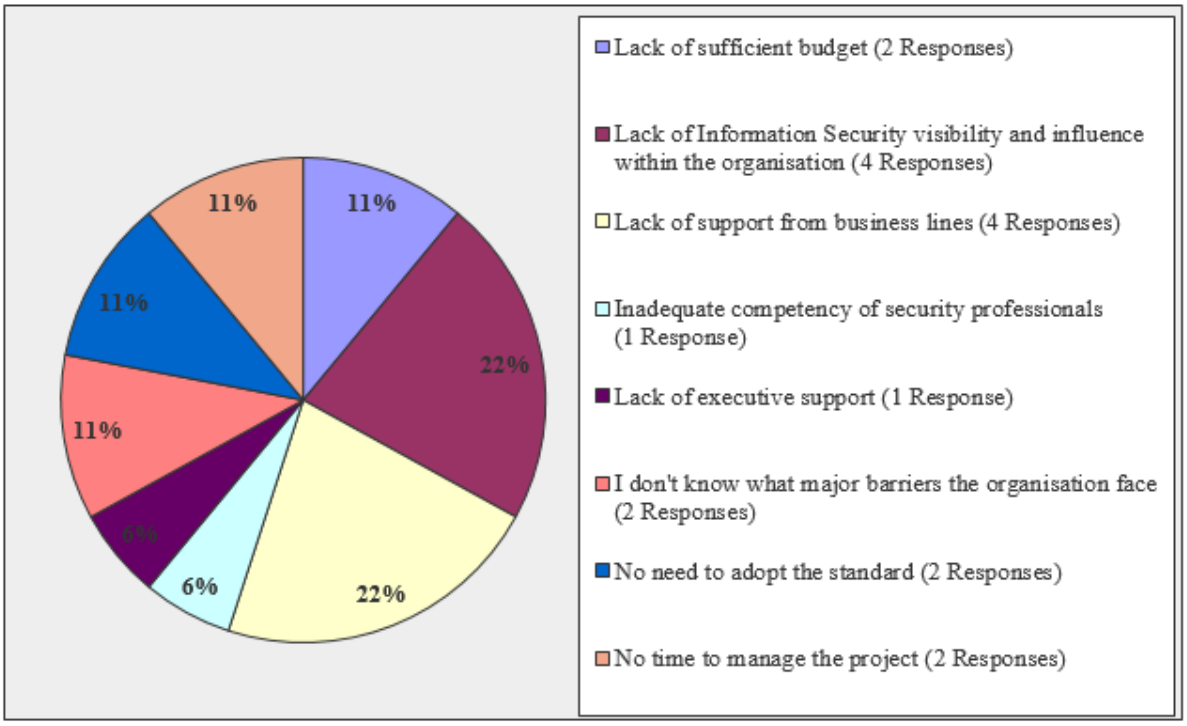

Figure 19: Barriers to ensure information security

Participants responded that they were challenged when adopting the ISO/IEC 27001 standard. Challenges organisations faced included maintaining the ISMS, understanding the standard, resources, senior management buy-in, and cultural change within the organisation. Figure 20 shows the main challenges organisations faced in adopting ISO/IEC 27001.

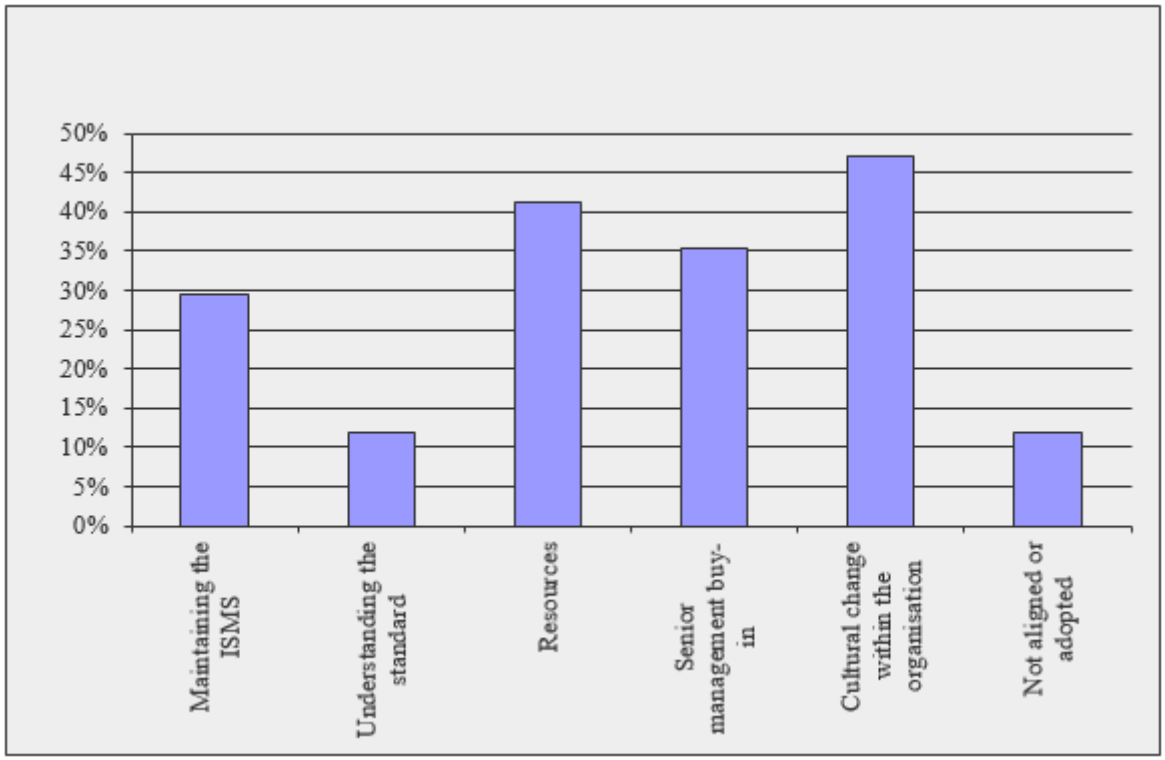

Figure 20: Challenges to adopt ISO/IEC 27001

The in-person interviews show that 53% of the organisations have an understanding of the ISMS certification process, whereas 57% responded that the organisations were either not aware of the ISMS certification process, or did not have the objective to understand the certification process. Results from the in-person interviews also show that 20% of the organisations have an understanding of the ISO/IEC 27002 standard, 13% responded that only IT resources that worked with the ISMS have an understanding of the ISO/IEC 27002 standard, and 67% of the organisations are not aware nor do they have an understanding of the ISO/IEC 27002 standard.

Based on the in-person interviews findings, organisations faced risks and issues when implementing the standard. Such risks and issues included budget constraints to implement security controls, the implementation was time consuming and took longer than anticipated, low awareness of the standard in the organisation, aligning and enforcing the standard between business and operations. Although none of these risks and issues caused a change in the strategy or stopped the adoption of the ISO/IEC 27001 standard, 13% did respond that their organisation has a new appreciation of the standard and the value it provided, as well as awareness that the board level assisted with support and backing for information security initiatives.

Analysis of the research findings shows that 28% responded that implementation would take more than 24 months to complete, with 6% of the responses suggesting that implementation would take less than 6 months as shown in Figure 21.

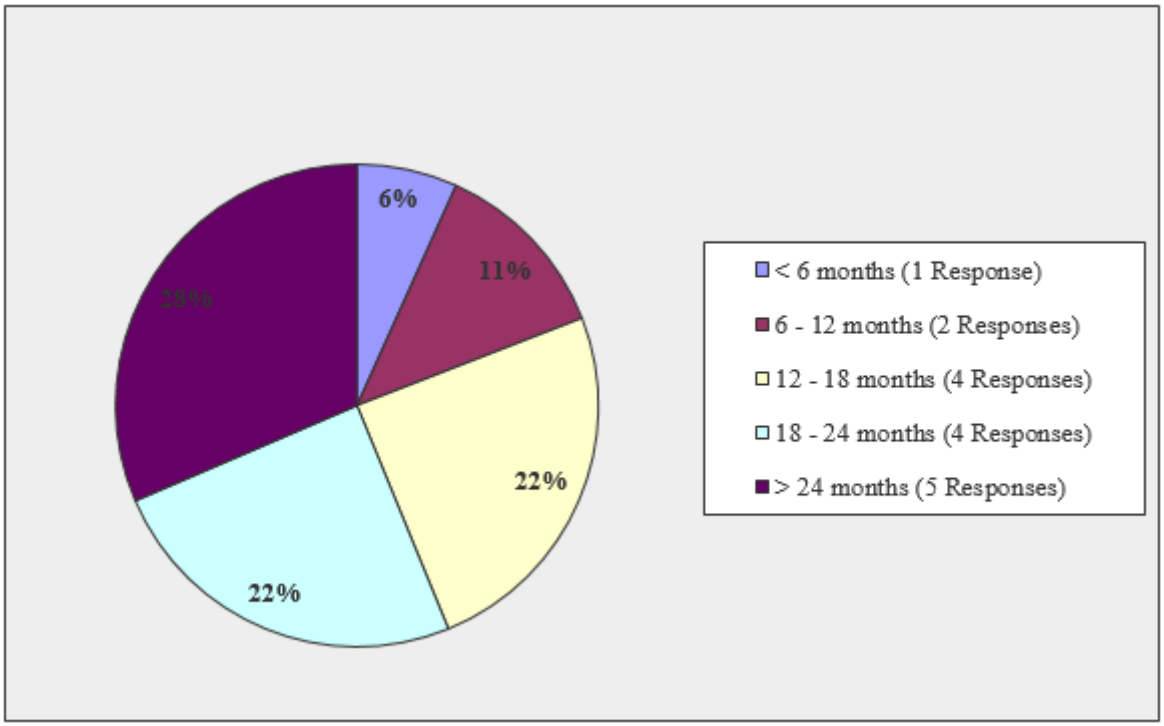

Figure 21: Timescale to implement ISO/IEC 27001

Based on the results, 78% of the participants responded that internal resources were used primarily to implement the ISMS, 11% responded that external resources such as consultants were used for implementation, and 11% of the participants did not respond.

Costs involved when implementing, receiving and maintaining the ISO/IEC 27001 certification included skilled resources who understood and were able to drive the agenda of information security, implementation of security controls that required procurement and maintenance of new technology and infrastructure, resource time and effort required to meet and implement the required policies and procedures, ISMS administration, and internal and external auditors fee.

The in-person interviews show that 53% of the organisations responded that if they were to implement ISO/IEC 27001 again, they would do the implementation differently. Participants responded that they would change how the risk assessment was done as from an asset perspective it was a long and tedious exercise, as well as the awareness approach of the ISO/IEC 27001 standard and the ISMS to staff members. Responses showed that more

research, planning, time, and skilled resources would have assisted in implementing the ISMS in a structured manner and more effectively. It also showed that there would be value to the implementation by driving information security governance from a senior management level and that senior management backing was the most critical aspect of a successful implementation. Majority of the responses showed that an expert in the ISO/IEC 27001 field would have assisted greatly in the implementation of the standard.

5.10.2 Analysis

Adoption of ISO/IEC 27001

Analysis of the research findings shows that there are a number of business objectives for adopting the ISO/IEC 27001 standard. Results show that almost a quarter of the organisations adopted ISO/IEC 27001 to ensure legal and regulatory compliance. Moreover, 11% of the business objectives involved a mandatory requirement from the organisation's holding company or customer base, and 44% involved the fact that the standard was recognised as an international best practice standard regarding the management of information security as shown in Figure 22.

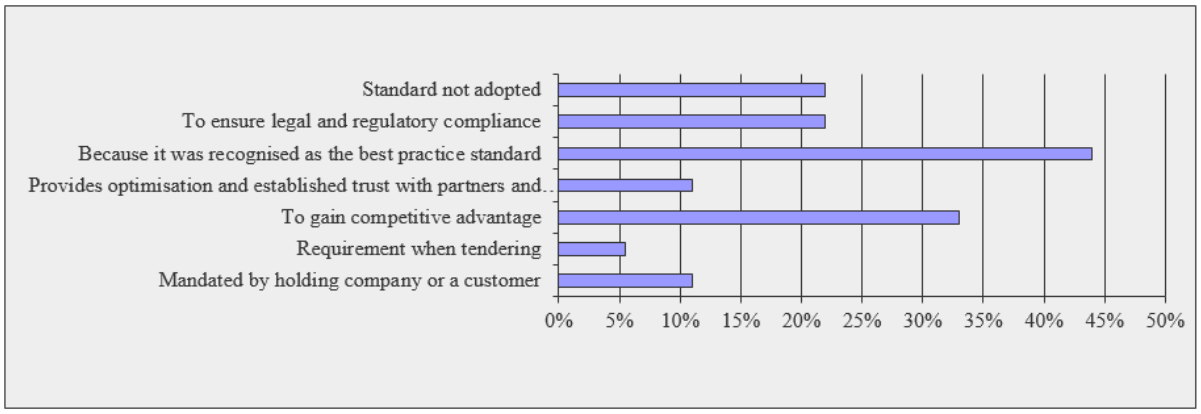

Figure 22: Objectives for adopting ISO/IEC 27001

Organisations with the objective to only align to the standard, did so because the alignment was mandated by the holding company or customers, provided a competitive edge, the standard was recognised as a best practice standard, it ensured legal and regulatory compliance, alignment provided optimisation, and established trust with partners and clients that information was being managed accordingly. Senior management's approval was obtained with the decisions to adopt, align to, as well as not adopt the standard.

Only organisations that have adopted the standard, have a developed and approved business case for the adoption of the standard implementation. Limited-to-no business cases were developed for organisations that are aligned to the standard. Senior management's support and commitment towards information security were also obtained by organisations that have adopted, as well as are aligned to the standard by establishing an information security policy and objectives and communicating the importance of meeting those objectives to the organisation. Organisations that have not adopted the standard did not obtain senior management support, nor was a business case developed to assist senior management with the decision.

Organisations that have adopted, or are aligned to the standard, have an ISMS implementation scope in place, whereas organisations that have not adopted the standard do not. Only organisations that have adopted the standard are completely aware of the mandatory documents required to comply for certification purposes, and have an SOA and a document control framework in place. There is limited knowledge of the mandatory ISMS documents or a SOA in place by organisations that are aligned to the standard as well as with organisations that have not adopted the standard. There is also limited drive from organisations that have not adopted the standard regarding the review process for documentation as documents are reviewed only if massive changes occur in the organisation. Organisations that have adopted, or are aligned to the standard review information security related documents on an annual or bi-annual basis, as well as when massive changes occur in the organisation.

The survey attempted to establish benefits that the adoption of the ISO/IEC 27001 standard provide to an organisation. Adoption provides the ability to identify and manage information security risks within the organisation, manage incidents more accordingly, while creating more awareness of information security. Adoption provides a market edge in the industry and drives business value to the organisation's customers and suppliers. Adoption of the standard makes senior management aware that information is an asset to the organisation that needs to be protected. Adoption of the ISO/IEC 27001 standard provides a better structure regarding information security within the organisation.

The main challenges organisations that have not adopted the standard face are senior management buy-in and support towards the program. Challenges organisations that have adopted, as well as are aligned to the standard face include an understanding of the ISO/IEC

27001 standard, resource skillset and availability required to maintain the ISMS, senior management buy-in and support towards the program, and being able to change the culture within the organisations regarding information security.

Organisations that have adopted the standard primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of between 6 to 24 months. Organisations that are aligned to the standard, primarily used internal resources, with minimal use of consultation services, and with an implementation timeline of between 6 months up to more than 24 months. Organisations that have not adopted the standard indicated that the estimate timeline for implementation would take a minimum of 6 months but a maximum of more than 24 months.

Organisation size

Analysis of the research findings shows that the business objectives for organisations of any size adopting the ISO/IEC 27001 standard are varied. These include that adoption provides a competitive advantage, the standard is recognised as a best practice standard and adoption ensures legal and regulatory compliance. In addition to these reasons, large organisations adopted the standard, as it was a requirement from their clients, whereas medium organisations adopted the standard as it provided a benefit when tendering for new business process. Apart from small organisations, senior management approval was obtained when making the decision to adopt as well as not to adopt the standard.

Medium and medium-to-large organisations that adopted the standard, had a business case (or were in the process of creating one) for the adoption of the standard. Limited-to-no business cases to assist senior management with the decision to adopt the standard were developed for small and large organisations.

Apart from limited-to-no senior management support and commitment towards information security by small organisations, medium, medium-to-large and large organisations obtained the support as senior management established an information security policy and objectives and communicated the importance of meeting these objectives to the organisation.

Based on the results, medium-to-large organisations dominated with 50% of the organisations surveyed have adopted the ISO/IEC 27001 standard. Medium-to-large and large organisations that adopted the standard, had an ISMS implementation scope and SOA in

place, whereas small and medium organisations that adopted the standard had limited-to-no scope or SOA in place. Apart from small organisations, medium, medium-to-large and large organisations had document control frameworks in place. Medium-to-large organisations were aware of the mandatory documents required to comply with the standard for certification purposes, whereas limited awareness by small, medium and large organisations existed.

Large, medium-to-large, and medium organisations that adopted the standard reviewed information security related documents on an annual or bi-annual basis, as well as when massive changes occurred in the organisation. Small organisations did limited-to-no review of information security related documents.

The adoption of the ISO/IEC 27001 standard throughout the various sized organisations created the ability to justify information security initiatives and projects and received the relevant senior management support thereof. Adoption enhanced the internal information security processes of the business, providing comfort to senior management that information security was being managed accordingly. Adoption provided more transparency regarding information security and awareness amongst employees regarding the ISMS and its requirements, and provided more awareness of how and who managed information security within the organisation.

The main challenge small organisations that adopted the standard faced was resources for the program, whereas small organisations that did not adopt the standard faced issues like senior management buy-in and support towards the adoption of the standard. Medium, medium-to-large, and large organisations faced challenges that included an understanding of the ISO/IEC 27001 standard, resource skillset and availability required to maintain the ISMS, senior management buy-in and support towards the program, and being able to change the culture within the organisations regarding information security to adopt the standard.

Small organisations primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of between 12 to 18 months. Medium organisations used primarily internal resources with additional consulting services when implementing the standard, with an implementation timeline of between 6 to 12 months. Medium-to-large and large organisations used primarily internal resources with

additional consulting services when implementing the standard, with an implementation timeline of between 12 to 24 months.

Industry

Analysis of the research findings showed that only organisations in the marketing and research and although limited, in the technology and data services industry, adopted the ISO/IEC 27001 standard. In addition to this, alignment to the ISO/IEC 27001 standard was made by organisations in the technology and data services, government, retail, financial, automotive, and health care industries.

Based on the results, business objectives for adopting the ISO/IEC 27001 standard for organisations in the various industries differed. Organisations in the marketing and research industry adopted the standard as it provided a competitive advantage and because the standard was recognised as an international best practice standard. Organisations in the technology and data services industry adopted the standard as it was a requirement from their clients, provided a benefit when tendering for new business process, provided a competitive advantage, the standard was recognised as an international best practice standard, and ensured legal and regulatory compliance. Government adopted the standard as the standard was recognised as an international best practice standard, and ensured legal and regulatory compliance. Organisations in the financial industry adopted that standard as it provided a competitive advantage, the standard was recognised as an international best practice standard, and ensured legal and regulatory compliance. Organisations in the automotive and health care industries adopted the standard because the standard was recognised as an international best practice standard. Apart from organisations in the professional membership industry, senior management approval was obtained with the decision to adopt as well as not adopt the standard.

Government and organisations in the marketing and research industry had a business case for the adoption of the standard, whereas organisations in the rest of the industries had limited-to-no business case in place. Organisations in the marketing and research, technology and data services, government, financials, and automotive industries obtained senior management support and commitment towards information security with the establishment of an information security policy and objectives and communicating the importance of meeting those objectives to the organisation. Limited-to-no senior management support towards

information security was obtained by organisations in the retail, health care and professional membership industries.

Organisations in the marketing and research, government, financials, and automotive industries which adopted the standard, had an ISMS scope in place, where limited-to-no scope was in place in organisations in the technology and data services, retail and professional membership industries. Organisations in the marketing and research, the technology and data services, and automotive industries, had a SOA in place, where government and organisations in the retail, financial, health care, and profession membership industries did not. Organisations in the marketing and research, government, health care, and professional membership, had a document control framework in place, where organisations in the technology and data services, retail, financial, and automotive did not.

Organisations in the marketing and research, retail, and automotive industries were aware of the mandatory documents required for certification purposes, whereas there was limited-to-no awareness by organisations in the technology and data services, government, financial, and professional membership industries.

The benefits of adopting ISO/IEC 27001througout the various industries included interest of potential customers, achieving new business, the organisation and business operation was aware of information security, a competitive edge, peer recognition, and client satisfaction. Adoption positioned the organisation better compared with competitors as the organisation operated in a more professional manner towards information security, and prepared the business with compliance towards the South Africa POPI Act. Adoption was used for marketing advantages and as evidence for proposal and tender submissions. Adoption also assured senior management that the organisation's information security was in place and managed accordingly.

Organisations in the various industries faced challenges with the adoption of the ISO/IEC 27001 standard. Organisations in the marketing and research industries faced senior management buy-in and support challenges towards the adoption of the standard, as well as challenges to change the culture within the organisations regarding information security. Government's main challenge was senior management buy-in and support towards the adoption of the standard, whereas health care faced challenges by resource skillset and availability required to maintain the ISMS. Organisations in the financial industry faced

senior management buy-in and support challenges as well as challenges to change the culture within the organisations regarding information security. Organisations in the retail, and technology and data services industries, faced challenges that consisted of senior management buy-in and support, an understanding of the ISO/IEC 27001 standard, resource skillset and availability required to maintain the ISMS, and being able to change the culture within the organisations regarding information security.

Organisations in the marketing and research industry used primarily internal resources with additional consulting services when implementing the standard, with an implementation timeline of between 12 to 18 months. Organisations in the technology and data services industry primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of 6 to more than 24 months. Organisations in the technology and data services industry primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of 6 to more than 24 months. The government primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of between 18 to 24 months. Organisations in the retail, financial, and health care industry primarily used internal resources with additional consulting services when implementing the standard, with an implementation timeline of more than 24 months. Organisations in the professional industry did not adopt the standard, but indicated that the implementation timeline would take more than 24 months.

5.11 Summary

As per the research method, a survey based on TAM was selected as the data collection method for this study and consisted of a web-based questionnaire and an in-person interview. This chapter explained the various sections in the web-based questionnaire and presented the findings as well as an analysis thereof for each section. Results of the in-person interviews were also given.

Chapter 6: Discussion of Survey Results

In this chapter, we discuss the findings and analysis of the following subsections of the survey: perceived usefulness of the ISO/IEC 27001 standard, attitude towards the use of the standard, social norms, performance expectancy, information security governance, information security risk management, organisation view of the standard, and adoption of the standard. We also propose a way forward for adoption of ISO/IEC 27001 in South Africa. In this section, we suggest what needs to happen to encourage adoption of the standard in South African organisations.

6.1 Perceived Usefulness

This section of the survey confirms that the South African organisations used in this study are aware of, and understand the perceived usefulness the ISO/IEC 27001 standard can provide such as improvement in work quality, as well as being able to provide more control and security over job functionality and enhance the effectiveness thereof.

6.2 Attitude Toward Use

Based on the results for this section of the survey, the South African organisations used in this study have a positive attitude towards the use of the ISO/IEC 27001 standard and the adoption thereof as it is seen to provide improved information security governance, compliance, security controls, and risk management for the organisation.

6.3 Social Norms

The South African organisations used in this study are aware of and understand the foundation that is required for the establishment of an ISMS according to the ISO/IEC 27001 standard, and that senior management accountability and support towards the establishment and implementation is critical for the success of the ISMS. Medium-to-large organisations, as well as organisations in the marketing, research and retail industries have the view that corporate governance, IT governance as well as information security governance do not have to be in place in order to establish a successful ISMS according to the ISO/IEC 27001 standard.

The views of the South African organisations used in this study are that ISO/IEC 27001 adoption should not be compulsory in the country. If, however, ISO/IEC 27001 adoption were compulsory, small organisations and organisations in the technology and data services industries would be further away from ISO/IEC 27001 compliance than larger sized organisations in various industries, as there is limited-to-no alignment done with the standard in these organisations. Small and medium-to-large organisations, as well as organisations in the technology and data services, government, financial, and health care industries would only adopt the standard if laws were put in place in the country, otherwise no action would take place to apply for certification.

6.4 Performance Expectance

Based on the results for this section of the survey, the participants agreed that adoption of the ISO/IEC 27001 standard would provide enhancement of job performance and efficiency within the organisation.

6.5 Information Security Governance

The South African organisations used in this study that are aligned with King III have a more stable foundation to ensure that information is adequately protected and that an ISMS is developed and implemented accordingly. Key elements for a successful ISMS include a governance structure for information security, an executive responsible for information security, an information security strategy, an information security policy, defined roles and responsibilities for information security within the organisation, and engagement levels for information security matters that include business and technology executives. A major barrier organisations face in ensuring information security is the lack of information security visibility and influence within the organisation as well as a lack of support from business lines.

6.6 Information Security Risk Management

Based on the results for this section of the survey, elements such as a risk methodology, a risk treatment plan, a risk treatment process, which is able to define which security controls should be implemented to mitigate an identified risk, a risk register that specifies information security related risks in place as well as an information security training and awareness programme are key to organisations that wish to adopt the ISO/IEC 27001 standard. Small

organisations, as well as organisations in the retail and government industries have a deficiency in their risk approach as well as information security training and awareness programme owing to elements such as risk methodology, a risk treatment process, and a risk register not being in place.

6.7 Organisation's View of ISO/IEC 27001

Based on the results for this section of the survey, the South African organisations used in this study are aware of the ISO/IEC and its available standards including ISO 9001, ISO 14001, ISO 31000, as well as ISO/IEC 27001. The organisations are also aware that the ISO/IEC 27001 standard has no limitations and was designed for adoption by any size organisation, in any industry. Management systems and standards such as ISO 9001, ISO 14001, ISO 20000-1, ITIL, COBIT, ISO 31000, ISO 27005, ISO 20252, and ISO 22301 are being used in conjunction with ISO/IEC 27001 in the sample organisations.

6.8 ISO/IEC 27001 Adoption

According to the participants in the survey, adoption enhances the internal information security processes of the business, providing comfort to senior management that information security is managed accordingly. Adoption provides more transparency regarding information security and awareness among employees regarding the ISMS and its requirements, and provides more awareness of how and who manages information security within the organisation. The adoption of the standard better positions organisations compared with competitors, as the organisations operate in a more professional manner towards information security, and are better prepared regarding the South Africa POPI Act requirements. Certification is used for marketing advantages and as evidence for proposal and tender submissions.

The survey findings highlighted the challenges faced by organisations in terms of adoption and alignment to the ISO/IEC 27001 standard. These challenges include an understanding of the ISO/IEC 27001 standard, resource skillset and availability required to maintain the ISMS within the organisation, senior management buy-in and support towards the program, and being able to change the culture within the organisations regarding information security.

6.9 The Way Forward for Adoption of ISO/IEC 27001 in South Africa

6.9.1 Advantages of Compliance

ISO/IEC 27001 adoption assists organisations in developing a globally recognised ISMS that can be independently audited for certification. Developing an ISMS based on ISO/IEC 27001 can assist South African organisations in meeting information security related regulatory compliance requirements including the South African POPI Act. Moreover, adopting ISO/IEC 27001 ensures that the relevant information security controls are in place, making organisations less vulnerable to data breaches.

Based on the survey results, ISO/IEC 27001 has been implemented in South African organisations, from small to large sized organisations, in various industries, ranging from alignment to the standard to adoption thereof. ISO/IEC 27001 is a management standard, not a technical standard, and was designed as a management system for implementing and maintaining information security appropriately. Such a framework enables an organisation to look at the information security elements within the context of the organisations, leadership and commitment, planning, support, operations, performance evaluation, and improvement of an ISMS.

Apart from the vast adoption of ITIL and COBIT, and the availability of ISO/IEC standards including ISO 9001, ISO 14001, ISO 31000, the sample organisations are aware of ISO/IEC 27001, and the usefulness and enhancement of performance and efficiency the standard provides. The ISO/IEC 27001 standard has no limitations and was designed for adoption by any size organisation, in any industry. There is a positive attitude towards the use of the standard within South Africa, as it would provide information security governance and compliance, security controls, and risk management improvement, but a different view towards ISO/IEC 27001 adoption, in that it should not be compulsory in the country. The objectives of organisations that have adopted the standard were that adoption ensured legal and regulatory compliance, and because the standard was recognised ISO/IEC 27001 as an international best practice standard regarding the management of information security.

ISO/IEC 27001 is an effective information security management approach. It was designed to be used as a baseline when establishing an ISMS within an organisation. Based on the survey results, adoption provides South African organisations the ability to identify and manage information security risks in the organisation, manage incidents more effectively, while

creating more awareness of information security in the organisation, as well as making senior management aware that information needs to be seen as an asset to the organisation that needs to be protected. Adoption provides a market edge in the industry and drives business value to the organisation's customers and suppliers.

6.9.2 Disadvantages of Not Being Compliant

Several key elements are required to implement successfully an ISMS based on the ISO/IEC 27001 standard. Based on the survey results, organisations that did not adopt the standard had less than half of the key elements in place required for compliance to the ISO/IEC 27001 standard. Not being compliant to the international standard creates the following disadvantages for an organisation:

- Lack of a structured corporate and information security governance structure;
- Lack of senior management accountability, support and commitment towards information security within the organisation;
- Non-existence of defined roles and responsibilities for information security within the organisation;
- Non-existence of a documented and approved information security strategy that actively engaged with both business and technology executives;
- No documented and approved information security policy in place;
- No active reporting of information security related matters to senior management;
- Lack of a documented and approved risk methodology, risk register, and risk treatment plan that identified actions, resources and funding, as well as responsibilities and priorities for managing information security risks;
- Non-existence of a documented and approved information security awareness program would not exist;
- Lack of a documented and approved document control framework;
- Lack of an ISMS implementation scope and SOA.

6.9.3 Steps to Follow in Order to Become Compliant

A foundation is required to implement an ISMS based on the ISO/IEC 27001 standard within an organisation, with the major element being senior management accountability and support towards the establishment and implementation of the standard. South African organisations that are aligned with King III have a more stable foundation to ensure that information is adequately protected and that an ISMS is developed and implemented appropriately.

Using the information obtained in this research, we have developed the following ISMS management guide. The guide is based on the ISO/IEC 27001 PDCA model (ISO/IEC 27001 2005), to assist organisations move towards ISO/IEC 27001 compliance and covers all the requirements currently not being met by organisations as per the research findings. Various other standards use the same high level PDCA approach (ISO 14000 2004; ISO 31000 2009; ISO 9000 2008; ITIL 2011), but this guide was developed to provide additional detailed steps required to successfully implement an ISMS based on ISO/IEC 27001 within an organisation.

Phase 1: Establishment of the ISMS program

This phase defines the steps that must be followed to establish an ISMS program.

- Establish and document the primary business objective from the organisation's mission and strategic planning, information security strategy, and IT goals, for developing and implementing an ISMS within the organisation and ensure that it aligns with the organisation's corporate governance structure.
- Develop and document the preliminary ISMS implementation scope. The preliminary ISMS implementation scope will indicate in which areas of the organisation the ISMS will be implemented in.
- Define and document the roles and responsibilities for information security within the organisation. This is to ensure that responsibilities for roles relevant to information security is defined within the organisation.
- Draft a business case and ISMS project proposal. The purpose of the business case and ISMS project proposal is to propose the implementation of an ISMS based on ISO/IEC 27001 to senior management. Conduct internal review of the business case and ISMS project proposal, and update accordingly.
- Obtain management support by conducting executive level review of the business case and ISMS project proposal. Management must make a commitment to the

establishment, planning, implementation, operation, monitoring, review, maintenance and improvement of the ISMS.

- Finalise and approve the business case and ISMS project.

Phase 2: Establishment of the ISMS

This phase defines the steps that must be followed to establish an ISMS.

- Define and integrate the organisation, IT, and physical environment scope and boundaries to develop and document the ISMS scope and boundaries for the implementation. Review, approve and publish the ISMS scope document.
- Define the information security requirements for the ISMS implementation to conduct a preliminary gap analysis. A gap assessment will report on items that needs to be addressed to in order to comply with ISO/IEC 27001. Produce and publish an ISMS gap analysis report.
- Establish the information security compliance obligations, framework for setting objectives, and evaluation criteria, to develop an information security documentation framework that consists of an information security policy, procedures, and control documentation that aligns with the organisation's strategic approach to information security risk management. Review, approve and publish the information security policy and documentation framework.
- Define and document a risk assessment approach by developing an information security risk methodology, developing criteria for accepting risks, and rating the severity of risks. Review, approve and publish the risk methodology.
- Prepare an inventory of information assets to protect and rank assets according to the risk criteria. The asset does not only have to include hardware and software, but could also include business operations and processes. Develop and publish a procedure for asset classification.
- Develop and publish a risk assessment plan based on the approved risk methodology. The plan will be used to identify, assess, and evaluate information security risks.
- Conduct a risk assessment to identify information security risks. Analyse and evaluate the identified risks. Decide to accept, transfer or reduce the identified risks. Define

and evaluate risk treatment options. Publish the information security risk assessment report.

- Identify and select the appropriate controls from ISO/IEC 27001 Annex A needed to mitigate the identified risks. Develop a draft information security risk treatment plan that identifies actions, resources and funding, as well as responsibilities and priorities for managing information security risks. Inform and obtain senior management acceptance of the residual risks. Obtain management authorisation and document management approval to implement the mitigating controls.
- Prepare the SOA document describing the controls that were selected from ISO/IEC 27001 Annex A, that are relevant and applicable to the ISMS, based on the results and conclusions of the information security risk assessment and risk treatment plan. Review, approve and publish the SOA document.

Phase 3: Implementation and operation of the ISMS

This phase defines the steps to follow for the implementation and operation of the ISMS.

- Formulate the final information security risk treatment plan that includes the actions, resources, funding, as well as responsibilities and priorities for managing information security risks and execute the plan.
- Implement the selected information security controls as stated in the SOA document, to meet the Annex A control objectives. Define how to measure the effectiveness of the selected controls to ensure that the controls are implemented effectively.
- Formulate the final organisational structure that includes the roles, responsibilities and reporting lines for information security. The updated organisational structure highlights management commitment to assign sufficient resources to manage, develop, maintain and implement the ISMS. Review, approve and publish the organisational structure.
- Identify the requirements for information security document and record control. Document and record management controls the format, access, and management of documents and records within the organisation. Develop document control and record control procedures. Review, approve and publish the document control and record control procedures.
- Workshop to develop and publish applicable information security policy driven control standards, technical standards and procedures based on the organisation's

structure, locations and assets. Control standards include standards such as logical access and encryption standards, whereas technical standards include standards such as firewall and router standards. Review, approve and publish the control standards, technical standards and procedures.

- Develop an information security awareness, training and education program. The program should cover what information security related content needs to be communicated, why it needs to be communicated, relevant stakeholders and their responsibilities, method of communication, as well as the format and frequency of communication. Review, approve, and launch the information security awareness, training and education program.
- Develop a procedure for management reviews of the ISMS. Management reviews should be conducted to allow senior management to discuss continual improvement, suitability, and effectiveness of the organisation's ISMS. Review, approve and publish the management review procedure.

Phase 4: Monitor and review the ISMS

This phase defines the steps that must be followed to monitor and review the ISMS.

- Formulate and execute monitoring and review procedures. Monitoring and review procedures are used for active reporting on information security related matters to senior management.
- Prepare planning, execution and documentation for the internal ISMS audit. Produce an information security corrective and preventive action report once the internal audit has been completed and address the findings.
- Contact an external auditor and arrange for an ISMS external assessment to be scheduled. Produce an information security corrective and preventive action report once the external assessment has been completed and address the findings.
- Initiate a compliance assessment to measure the effectiveness of the implemented information security controls to verify that security requirements have been met.
- Plan and conduct a review of the information security risk assessment and management reviews of the implemented ISMS. This is to ensure that the risk assessment and management review are appropriate and effective.

- Update the organisation's information security plans to take account of monitoring and reviewing as well as record actions and events that have an impact on the implemented ISMS.

Phase 5: Maintain and improve the ISMS

This phase finally defines the steps to follow to maintain and improve the implemented ISMS.

- Implement improvements that were identified in the external and internal audits throughout the ISMS.
- Develop a corrective actions procedure and preventative actions procedure. The corrective and preventative procedures are developed to assign responsibilities which will initiate, request, implement and verify the effectiveness of the corrective and preventative actions. Review, approve and publish the corrective actions procedure and preventive actions procedure.
- Perform appropriate corrective and preventative actions of identified non-conformities and communicate the actions and the improvements to the relevant stakeholders. Ensure that the actions and improvements achieve the intended objectives.
- Conduct periodic compliance assessment to confirm that the ISMS continues to operate as specified and intended.
- Contact an external certification body to arrange the certification audit for the implemented ISMS. The audit consists of three stages. Stage one is an informal review of the ISMS that includes checking the existence and completeness of key documents such as the ISMS scope and SOA to determine the scope content of the ISMS. Stage two is an independent test of the ISMS against the requirements specified in ISO/IEC 27001. Stage three is a follow-up review or periodic audit to confirm that the organisation remains in compliance with the standard.

6.10 Summary

In this chapter we summarized the results and analyses of the survey findings. Based on the findings, the South African organisations used in this study are aware of, and understand the perceived usefulness the ISO/IEC 27001 standard. We presented a section on the way forward for the adoption of ISO/IEC 27001 in South Africa. In this section we discussed the

advantages of compliance and the disadvantages of non-compliance with ISO/IEC 27001 as well as the steps to follow, based on the ISO/IEC 27001 PDCA model, to become compliant with the international standard.

Chapter 7: Conclusion and Future Work

This study explored various organisation sizes and industries to investigate the adoption of ISO/IEC 27001 in South Africa. The general theoretical literature on this subject and specifically in the context of South Africa is inconclusive on several vital questions. The study sought to answer the following question:

Why is the adoption of the ISO/IEC 27001 standard low in South Africa?

This conclusion chapter presents the research conclusion, a summary of contributions, and suggestions for further research.

7.1 Conclusion

The main objective of this study was to investigate the adoption of ISO/IEC 27001 within South African organisations. This study led to a reasonable conclusion on the adoption of ISO/IEC 27001 within the South African organisations used in this study. The conclusion is spread across the findings of the designed and achieved research subobjectives.

The first objective of this research was to determine what knowledge South African organisations have of the ISO/IEC 27001 standard. The conclusion reached is that organisations that participated in this study have an understanding of the ISO/IEC 27001 standard. South African organisations understand the usefulness of the standard as it provides improved work quality, as well as control and security over job functionality. South African organisations have a positive attitude towards the use of the ISO/IEC 27001 standard as it enhances the overall information security posture of an organisation by improving information security governance and compliance, security controls, and risk management elements within the organisation. The sample organisations understand the fundamental foundation elements required for the adoption of the ISO/IEC 27001 standard, and that senior management accountability and support towards the establishment and implementation is critical for successful adoption.

The second objective was to determine which organisations have adopted the ISO/IEC 27001 standard in South Africa. The conclusion is that less than a quarter of South African organisations have fully adopted the ISO/IEC 27001 standard. Organisations that have adopted the standard, are those in the marketing and research, and technology and data

services industries. From an organisation size perspective, medium-to-large sized organisations have adopted the standard. Half of the South African organisations surveyed are aligned to ISO/IEC 27001, rather than having adopting it, as only elements of the standard (specifically the Annex A portions of the standard) are used within the organisation, and registration of the standard implementation is not a business objective.

A third objective was to determine the business objective(s) in adopting the ISO/IEC 27001 standard. The conclusion is that the main business objectives for adopting the ISO/IEC 27001 standard are:

- to ensure legal and regulatory compliance within the organisation;
- to fulfil a requirement from the organisation's holding company or a customer;
- that ISO/IEC 27001 is an international best practice standard regarding the management of information security.

The fourth objective for this research was to evaluate the benefits gained by organisations that had adopted ISO/IEC 27001. The conclusion reached is that organisations gain several benefits from adopting the standard or even purely aligning with ISO/IEC 27001. Benefits include:

- Enabling the organisation to identify and manage information security risks, as well as information security incidents more effectively;
- Providing a better structure regarding information security within the organisation;
- Making the organisation's senior management aware that information needs to be seen as an asset to the organisation that needs to be protected.
- Providing a market edge in the industry and driving business value to the organisations customers and suppliers;
- Enhancing the internal information security processes of the business, providing comfort to senior management that information security is managed accordingly in the organisation;
- Providing more transparency regarding information security and awareness among employees of the ISMS and its requirements, and more awareness of how and who manages information security within an organisation;
- Acting as a compliance element with respect to the South Africa POPI Act.

The final objective was to evaluate the challenges faced by organisations that have adopted ISO/IEC 27001. The conclusion is that organisations face several challenges with respect to adoption, or even aligning with ISO/IEC 27001. Challenges include:

- An understanding of the ISO/IEC 27001 standard flow and requirements when implementing the standard within an organisation;
- The resource skillset and availability required to maintain the ISO/IEC 27001 ISMS within the organisation;
- Senior management buy-in and support towards ISO/IEC 27001 adoption;
- Being able to change the culture within the organisations regarding information security.

The overall conclusion is that although there is a vast knowledge of ISO/IEC 27001 in the sampled organisations, there is limited adoption of the standard. The objectives of organisations that adopted the standard, were to ensure legal and regulatory compliance, and to fulfil client requirements. Adoption does provide several benefits to an organisation by providing a market edge for the organisation in the industry and driving business value to the organisations customers and suppliers. However, adoption also has its challenges, with the main challenge being able to change the culture within the organisation regarding information security.

Organisations that participated in this study tend to rather align to ISO/IEC 27001, as there is no business objective to register the ISMS implementation and receive certification for the adoption, but rather because ISO/IEC 27001 is an international best practice standard regarding the management of information security. To align to the standard does not provide the benefit of using the registration certificate as a marketing tool, but does assist in a better structure and management of information security within the organisation. The main challenge organisations have when pursuing adoption though is senior management buy-in and support towards the ISO/IEC 27001 adoption.

7.2 Summary of Contributions

This research has led to four primary contributions, which are summarised as follows:

- As per the 2012 ISO Survey (ISO 2012) that includes the world distribution of ISO/IEC 27001 certificates, it clearly shows the limited adoption of ISO/IEC 27001 in

South Africa. For this research, we investigated the adoption of ISO/IEC 27001 within South African organisations and generated information that illustrated the knowledge the organisations that participated in this study have of the ISO/IEC 27001 standard. The research also generated information of which organisations (of various sizes and industries) in South Africa had adopted the ISO/IEC 27001 standard, as well as the business objective(s) established for the adoption of the ISO/IEC 27001 standard.

- The research provides a view of the key elements required for the successful adoption of ISO/IEC 27001 within an organisation, as well as the realised benefits and challenges arising from adoption. Additionally, with such key elements identified the adoption of ISO/IEC 27001 by organisations can now be established and implemented more easily.
- The investigation of the adoption of ISO/IEC 27001 in South Africa is believed to be the first investigation of its kind. This research can be expanded in the future to develop an ISMS implementation guideline to assist senior management in establishing an information security strategy and framework with the aim to adopt the ISO/IEC 27001 standard within the organisation.
- An ISMS management guide based on the ISO/IEC 27001 PDCA model has been developed as part of this research to help organisations interested in adopting the standard, move towards ISO/IEC 27001 compliance.

7.3 Suggestions for Further Research

This study was conducted with a relatively small audience in a limited timescale to find preliminary results; as such, the research provides a starting point of the status of ISMSs specifically aimed at the ISO/IEC 27001 standard within a South African context.

The following investigations can be conducted to extend this research:

- Investigation of ISO/IEC 27001 adoption with a larger audience over a longer timescale to evaluate the adoption of ISO/IEC 27001 throughout the entire South Africa.
- A detailed investigation to establish the effectiveness of the ISMSs of organisations that have adopted ISO/IEC 27001.

- A detailed investigation to establish the effectiveness of an organisations information security risk treatment control selection and implementation.
- A detailed investigation to establish how organisations are measuring and monitoring the compliance of implemented information security controls.

As the investigation of the adoption of ISO/IEC 27001 in South Africa is believed to be the first of its kind, additional research may be required to escalate its comprehensiveness and to evaluate its impact and effectiveness.

References

AENOR, 2004. Asociación Española de Normalización y Certificación (AENOR) UNE 71502:2004. Available at: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?codigo=N0030656&tipo=N [Accessed March 27, 2014].

Arnason, S.T. & Willett, K.D., 2007. *How to Achieve 27001 Certification: An Example of Applied Compliance Management*, CRC Press.

AS/NZS 7799.2, 2003. *Standards Australia, AS/NZS 7799.2:2003 Information security management, Part 2: Specification for information security management systems*, Standards Australia/Standards New Zealand International.

Basel, 2010. *Basel Committee on Banking Supervision Principles for enhancing corporate governance*, Bank for International Settlements.

Van Bon, J., 2006. *Frameworks for IT Management*, Van Haren Publishing.

BS 7799-1, 1999. *Information Security management Code of practice for Information Security Management*, British Standards Institution.

BS 7799-2, 1999. *Information security management. Specification for information security management systems*, British Standards Institution.

BS 7799-2, 2002. *Information security management. Specification with guidance for use*, British Standards Institution.

BSI, 2012. Benefits of ISO/IEC 27001 Information Security Research Report Summary. Available at: http://www.bsigroup.ae/upload/CaseStudiesM/Benefits of ISOIEC 27001 Information Security Research Report SummaryResearch_Summary.pdf [Accessed September 16, 2013].

BSI, 2013. ISO/IEC 27001 - Information Security Management - Transition guide. Available at: http://www.bsigroup.com/1564A3CD-A1A0-411B-9224-4CFB3CFA2F60/FinalDownload/DownloadId-C246AC1E4AEFF1B5C5660C5DD80474C3/1564A3CD-A1A0-411B-9224-4CFB3CFA2F60/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf [Accessed April 1, 2014].

CA, 2008. *COMPANIES ACT 71 OF 2008*, Department: Justice and Constitutional Development , Republic of South Africa. Available at: http://www.justice.gov.za/legislation/acts/2008-071amended.pdf [Accessed March 3, 2014].

Cadbury, 1992. *The Cadbury Report - The Cadbury Archive*, Professional Publishing.

Calder, A., 2009. *Information Security Based on ISO 27001/ISO 27002: A Management Guide*, Van Haren Publishing.

Check, J. & Schutt, R.K., 2012. *Research Methods in Education*, SAGE Publications.

Chew, E., Swanson, M., Stine, K.M., Bartol, N., Brown, A. & Robinson, W., 2008. *Special Publication 800-55 Rev. 1, Performance Measurement Guide for Information Security*, National Institute of Standards and Technology.

COBIT, 2012. *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT*, Information Technology Governance Institute.

Craft, R., Wyss, G., Vandewart, R. & Funkhouser, D., 1998. An Open Framework for Risk Management. *National Institute of Standards and Technology*. Available at: http://csrc.nist.gov/nissc/1998/proceedings/paperE6.pdf [Accessed March 11, 2014].

Davis, F.D., 1986. *A technology acceptance model for empirically testing new end-user information systems : theory and results*. Massachusetts Institute of Technology.

Dillard, K., Pfost, J. & Stephan, R., 2006. The Security Risk Management Guide. *Microsoft*. Available at: http://www.microsoft.com/en-za/download/details.aspx?id=6232 [Accessed March 17, 2014].

Dillman, D.A., Smyth, J.D. & Christian, L.M., 2008. *Internet, Mail, and Mixed-Mode Surveys: The Tailored Design Method, 3rd Edition*, John Wiley & Sons.

DPA, 1978. *France Data Protection Act of 1978 (revised in 2004)*, French Republic government. Available at: http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/ [Accessed January 13, 2014].

DPA, 1998. *United Kingdom Data Protection Act 1998*, United Kingdom government. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed January 13, 2014].

DTI, 2000. UK Department of Trade and Industry's (DTI) Managing Information Security solutions from the UK. Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/industry_files/pdf/solutions.pdf [Accessed March 25, 2014].

Duck, S. & McMahan, D.T., 2012. *The Basics of Communication: A Relational Perspective: Second Edition*, SAGE Publications.

Eloff, M. & von Solms, S., 2000. Information Security Management: A Hierarchical Framework for Various Approaches. *Computers & Security*, 19(3), pp. 243–256.

FDPA, 2001. *Germany Federal Data Protection Act of 2001*, German government. Available at: http://www.iuscomp.org/gla/statutes/BDSG.htm [Accessed January 13, 2014].

Feng, N., Wang, H.J. & Li, M., 2014. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256, pp. 57–73.

Forbes, 2008. Bernie Madoff's $50 Billion Ponzi Scheme - Forbes. *Forbes*. Available at: http://www.forbes.com/2008/12/12/madoff-ponzi-hedge-pf-ii-in_rl_1212croesus_inl.html [Accessed March 3, 2014].

Forbes, 2009. The Satyam Scandal - Forbes. *Forbes*. Available at: http://www.forbes.com/2009/01/07/satyam-raju-governance-oped-cx_sb_0107balachandran.html [Accessed March 3, 2014].

Fricker, R.D.J. & Schonlau, M., 2002. Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature. *SAGE Publications*, 14(4), pp. 1–23.

Goosen, R. & Rudman, R., 2013. The development of an integrated framework in order to address King III 's IT governance principles at a strategic level. *South African Journal of Business Management*, 44(4), pp. 91–103.

Guan, J., Lei, M., Zhu, X. & Liu, J., 2013. Knowledge-based information security risk assessment method. *The Journal of China Universities of Posts and Telecommunications*, 20, pp. 60–63.

Hufstedler, S.M. & Hancock, T., 2006. *Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition*, Information Technology Governance Institute.

Humphreys, E., 2008. Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4), pp. 247–255.

IEC 31010, 2009. *IEC 31010:2009 - Risk management -- Risk assessment techniques*, International Organization for Standardization.

InternetWorldStats, 2012. Africa Internet Usage, Facebook and Population Statistics. Available at: http://www.internetworldstats.com/stats1.htm#africa [Accessed September 16, 2013].

Investopedia, 2009. Case Study: The Collapse of Lehman Brothers. *Investopedia*. Available at: http://www.investopedia.com/articles/economics/09/lehman-brothers-collapse.asp [Accessed March 3, 2014].

IoDSA, 2009. Institute of Directors in Southern Africa (IODSA) KING Code of Governance for South Africa. Available at: http://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iii/king_code_of_governance_for_.pdf [Accessed March 3, 2014].

ISACA, 2008. *Aligning COBIT 4.1, ITIL V3 and ISO / IEC 27002 for Business Benefit. A Management Briefing From ITGI and OGC*, ISACA.

ISACA, 2011. Global Status Report on the Governance of Enterprise IT. *ISACA*. Available at: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/global-status-report-on-the-governance-of-enterprise-it-geit-2011.aspx [Accessed April 10, 2014].

ISECT, 2014. ISO 27001 Timeline. Available at: http://www.iso27001security.com/html/timeline.html [Accessed April 28, 2015].

ISF, 2013. Information Security Forum (ISF), The Standard of Good Practice for Information Security. Available at: https://www.securityforum.org/shop/p-71-173 [Accessed March 18, 2014].

ISO, International Electrotechnical Commission. Available at: http://www.iso.org [Accessed September 16, 2013].

ISO, 2012. ISO Survey. Available at: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC 27001 [Accessed April 10, 2014].

ISO 14000, 2004. *ISO 14000 - Environmental management*, International Organization for Standardization.

ISO 31000, 2009. *ISO 31000 - Risk Management — Principles and guidelines*, International Organization for Standardization.

ISO 9000, 2008. *ISO 9000 - Quality Management*, International Organization for Standardization.

ISO/IEC 17799, 2000. *Information technology -- Code of practice for information security management*, International Organization for Standardization.

ISO/IEC 27001, 2005. *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements*, International Organization for Standardization.

ISO/IEC 27001, 2013. *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements*, International Organization for Standardization.

ISO/IEC 27002, 2005. *ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management*, International Organization for Standardization.

ISO/IEC 27002, 2013. *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*, International Organization for Standardization.

ISO/IEC 27003, 2010. *ISO/IEC 27003:2010 Information technology -- Security techniques -- Information Security management system implementation guidance*, International Organization for Standardization.

ISO/IEC 27005, 2011. *ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management*, International Organization for Standardization.

ISO/IEC 38500, 2008. *ISO/IEC 38500:2008 - Corporate governance of information technology*, International Organization for Standardization.

ITGI, Information Technology Governance Institute. *Information Technology Governance Institute*. Available at: http://www.itgi.org/Template_ITGI.html [Accessed March 3, 2014].

ITIL, 2011. *ITIL Lifecycle Publication Suite*, The Stationery Office.

Kelley, K., Clark, B., Brown, V. & Sitzia, J., 2003. Good practice in the conduct and reporting of survey research. *International journal for quality in health care : Journal of the International Society for Quality in Health Care / ISQua*, 15(3), pp. 261–266.

Khanmohammadi, K. & Houmb, S.H., 2010. Business Process-Based Information Security Risk Assessment. In *2010 Fourth International Conference on Network and System Security*. IEEE, pp. 199–206.

Kneuper, R., 2008. *CMMI: Improving Software and Systems Development Processes Using Capability Maturity Model Integration*, Rocky Nook.

Kosutic, D., 2010. Problems with defining the scope in ISO 27001. Available at: http://blog.iso27001standard.com/?s=scope&x=0&y=0&lang=en [Accessed April 8, 2014].

Kosutic, D., 2014. Why is management review important for ISO 27001 and ISO 22301? Available at: http://blog.iso27001standard.com/?s=scope&x=0&y=0&lang=en [Accessed April 8, 2014].

Kouns, J. & Minoli, D., 2011. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*, John Wiley & Sons.

Lund, M.S., Solhaug, B. & Stølen, K., 2011. *Model-Driven Risk Analysis - The CORAS Approach*, Springer.

Mayer, N., Heymans, P. & Matulevičius, R., 2006. Design of a Modelling Language for Information System Security Risk Management. *CiteSeerx*, pp. 121–132.

Moeller, R.R., 2007. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework*, Wiley.

NIST, 2012. Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. *National Institute of Standards and Technology*, (September). Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf [Accessed March 14, 2014].

NIST, 2010. Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems. *National Institute of Standards and Technology*, (February). Available at:

http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [Accessed March 27, 2014].

NIST, 2011. Special Publication 800-39, Managing Information Security Risk. *National Institute of Standards and Technology*, (March). Available at: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf [Accessed March 27, 2014].

Ntim, C.G., 2013. An Integrated Corporate Governance Framework and Financial Performance in South African-Listed Corporations. *South African Journal of Economics*, 81(3), pp. 373–392.

PA, 1988. *Australia Privacy Act 1988*, Attorney-General's Department, Australian government. Available at: http://www.comlaw.gov.au/Details/C2014C00757 [Accessed January 13, 2014].

Panda, P., 2009. Feature The OCTAVE Approach to Information Security Risk Assessment. *ISACA*, 4, pp. 1–5.

Parkin, S.E., van Moorsel, A. & Coles, R., 2009. An information security ontology incorporating human-behavioural implications. In *Proceedings of the 2nd iIternational Conference on Security of Information and Networks - SIN '09*. New York, New York, USA: ACM Press, pp. 46–55.

Poore, R.S., 2006. *Information Security Management Handbook, Fifth Edition, Volume 3*, CRC Press.

POPI, 2013. *South Africa Protection of Personal Information Act*, Department: Justice and Constitutional Development, Republic of South Africa. Available at: http://www.justice.gov.za/legislation/acts/2013-004.pdf [Accessed January 13, 2014].

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

SABS, 2014a. South African Bureau of Standards - Certification and Accreditation. *South African Bureau of Standards*. Available at: https://www.sabs.co.za/Certification/certification_schemesearch2.asp?Code=SANS 27001 [Accessed May 26, 2014].

SABS, 2014b. South African Bureau of Standards - Numerical List Of Standards. *South African Bureau of Standards*. Available at: https://www.sabs.co.za/Standard-Sales/docs/Numerical_list_(SABS).pdf [Accessed March 27, 2014].

Saint-Germain, R., 2005. Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*, 39(4).

Shamala, P., Ahmad, R. & Yusoff, M., 2013. A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), pp. 45–52.

Shedden, P., Scheepers, R., Smith, W. & Ahmad, A., 2011. Incorporating a knowledge perspective into security risk assessments. *VINE*, 41(2), pp. 152–166.

Shedden, P., Scheepers, R., Smith, W. & Ahmad, A., 2009. *Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study*, Available at: http://aisel.aisnet.org/acis2009/96 [Accessed March 11, 2014].

Shedden, P., Smith, W. & Ahmad, A., 2010. Information Security Risk Assessment : Towards a Business Practice Perspective. *Australian Information Security Management Conference*, (November).

Siig, J.E., 2013. How to develop a Statement of Applicability (SOA) according to ISO/IEC 27001:2013. *Neupart*. Available at: http://www.slideshare.net/Neupart/how-to-develop-a-statement-of-applicability-according-to-iso-27001-2013 [Accessed April 8, 2014].

Sills, S.J. & Song, C., 2002. Innovations in Survey Research: An Application of Web-Based Surveys. *Social Science Computer Review*, 20(1), pp. 22–30.

Sincero, S.M., 2014. The Survey Guide. *Explorable*. Available at: https://explorable.com/course/the-survey-guide [Accessed May 25, 2014].

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

Von Solms, S.H. (Basie), 2005. Information Security Governance – Compliance management vs operational management. *Computers & Security*, 24(6), pp. 443–447.

SOX, 2002. *Public Law 107 – 204 107th Congress An Act*, United States of America government. Available at: https://www.sec.gov/about/laws/soa2002.pdf [Accessed March 3, 2014].

Stawarski, C. & Phillips, P.P., 2008. *Data Collection: Planning for and Collecting All Types of Data*, John Wiley & Sons.

Straub, D.W., 1989. Validating Instruments in MIS Research. *MIS Quarterly*, 13(2), pp. 147–169.

Swanson, M. & Guttman, B., 1996. Generally Accepted Principles and Practices for Securing Information Technology Systems. *National Institute of Standards and Technology*, (September). Available at: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf [Accessed March 20, 2014].

Thissen, M.R., 2013. Computer Audio-Recorded Interviewing as a Tool for Survey Research. *Social Science Computer Review*, 32(1), pp. 90–104.

Tshinu, S., Botha, G. & Herselman, M., 2008. An Integrated ICT Management Framework for Commercial Banking Organisations in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, 3, pp. 40–53.

Turnbull, 1999. *Internal Control, Guidance for Directors on the Combined Code*, The Institute of Chartered Accountants in England & Wales.

VALIT, 2008. *Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0*, ISACA.

Veiga, A. Da & Eloff, J.H.P., 2007. An Information Security Governance Framework. *Information Systems Management*, 24(4), pp. 361–372.

Verizon, 2013. Data breach investigations report. *Verizon*. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [Accessed September 16, 2013].

Wright, M., 1999. Third generation risk management practices. *Computer Fraud & Security*, 1999(2), pp. 9–12.

Yazar, Z., 2012. A Qualitative Risk Analysis and Management Tool - CRAMM. *SANS Institute*. Available at: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 [Accessed March 14, 2014].

Yildirim, Y.E., Akalp, G., Aytac, S. & Bayram, N., 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4), pp. 360–365.

Ying Chen, 2005. Information Valuation for Information Lifecycle Management. In *Second International Conference on Autonomic Computing (ICAC'05)*. IEEE, pp. 135–146.

Appendix A – Web based Questionnaire

SECTION 1 GENERAL		
1	What is your age?	a) Under 20 b) Between 20 and 30 c) Between 31 and 45 d) Above 45
2	What is the highest level of education you have completed?	a) High school b) Diploma c) Bachelor d) Master e) PhD f) Other
3	Which of the following best describes the principal industry of your organization?	a) Basic Materials b) Consumer Goods and Service c) Financials d) Health Care e) Industrials f) Media g) Retail h) Telecommunications i) Technology and data services j) Marketing and Research k) Tourism k) Other
4	Your organisation size?	a) < 50 employees b) 50 - 200 employees c) 200 - 2000 employees c) > 2000 employees

SECTION 2 PERCIEVED USEFULNESS		
5	ISO/IEC 27001 will improve the quality of my work	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
6	ISO/IEC 27001 will make it easier for me to do my job	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
7	ISO/IEC 27001 will make it faster for me to do my job	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
8	ISO/IEC 27001 will give me better control over my job	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
9	ISO/IEC 27001 will enhance my effectiveness	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
10	ISO/IEC 27001 will enable me to do my job more securely	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree

SECTION 3 ATTITUDE TOWARDS USE		
11	I think that ISO/IEC 27001 certification is beneficial for my organization. (Provides compliance; provides integrity of data records; help maintain access controls to valuable material for which the company controls copyright; privacy of customers and employees; etc.)	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
12	I think that ISO/IEC 27001 certification will improve my organization's information security controls, risk management, compliance and information security governance.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
13	I think that ISO/IEC 27001 certification is unnecessary for my organization.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
SECTION 4 SOCIAL NORMS		
14	Select the options that should be implemented first to establish information security management system in your organization?	a) Information Security governance b) ISO/IEC 27001 c) Legal infrastructure d) Corporate governance e) Information Technology governance d) None

15	Do you agree that ISO/IEC 27001 certification should be compulsory in our country?	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree

16	Who do you think should be responsible from obtaining ISO/IEC 27001 certificate and establishing information security management system?	a) Senior management b) IT c) Consultants d) All organization employees e) I don't know

17	Suppose that ISO/IEC 27001 certification is compulsory in our country, which option would be true for you?	a) I meet all of the requirements of ISO/IEC 27001 on paper since it is a must, however my method in doing b) I do my job concerning that both ISO/IEC 27001 is a must and it brings effectiveness to my job. c) ISO/IEC 27001 is not applied in my organization even on paper assuming that it is a must in our country.

18	Unless laws are first put in place to establish an Information Security Management System (ISMS) in my organization, no notice will be take of this certification.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree

SECTION 5 PERFORMANCE EXPECTANCY

19	I think that there will be a decrease in my performance when ISO/IEC 27001 certification comes to my organization.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
20	I think that both job performance and ISO/IEC 27001 can be driven together.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree
21	I think that carrying out my job efficiently and ISO/IEC 27001 can be driven together.	a) Strongly agree b) Agree c) Neutral d) Disagree e) Strongly disagree

SECTION 6 INFORMATION SECURITY GOVERNANCE

22	The release of the third King Report on Corporate Governance (King III) in 2009 highlighted the requirements and implementation of more effective information technology governance principles due to the changing nature of information technology environments in organisations. Does your organisation comply with the King 3 report?	a) Yes b) No c) I don't know d) Somewhat

23	King III includes a section on information security, where the board of an organisation is required to ensure that information is adequately protected and that an Information Security Management System (ISMS) is developed and implemented. If the organisation complies with King 3, has an ISMS been developed and implemented?	a) Yes b) No c) I don't know
24	Are the Roles and responsibilities for information security (IS) in the organization defined?	a) Yes b) No c) I don't know
25	Does the organisation have a documented and approved governance structure for information security?	a) Yes b) No c) I don't know
26	Does your organisation have an executive(s) responsible for information security?	a) Yes b) No c) I don't know
27	Who does the executive(s) responsible for information security in the first instance report to?	a) Board of Directors b) Chief Executive Officer (CEO) c) Chief Information Officer (CIO) d) Chief Technology Officer (CTO) e) Chief Operations Officer (COO) f) Chief Financial Officer (CFO) g) Group Risk Officer (GRC) h) Internal Audit i) Legal and Compliance j) Information Security Committee k) Other

28	Select which functions are within the scope of the executive(s) responsible for information security?	a) Information security governance b) information security strategy and planning c) Human resource security d) Asset management e) Access control f) Cryptography g) Physical and environmental security h) Operations security i) Communications security j) System acquisition, development and maintenance k) Supplier relationships l) Information security incident management m) Information security aspects of business continuity management n) Information security Compliance o) Information Security Risk assessments p) Other

29	Does your organisation have a documented and approved information security strategy?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

30	Does your organisation actively engage both line of business and technology executives in identifying requirements for the organisations information security strategy?	a) Lines of business executives only b) Technology executives only c) Both lines of business and technology executives d) Neither lines of business nor technology executives e) I don't know

31	Is there an approved information security policy that includes a framework for setting objectives, takes into account contractual, legal and regulatory requirements, aligns with the information security risks to the business and establishes the criteria for risk evaluation?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

32	What major barriers does the organisation face in ensuring information security?	a) Lack of sufficient budget b) Lack of Information Security visibility and influence within the organisation c) Lack of support from business lines d) Lack of clarity on Information Security mandate, roles and responsibilities e) Lack of documented barriers f) Inadequate competency of security professionals g) Lack of Information Security strategy h) Lack of executive support i) Inadequate functioning and/or inoperability of security products j) Other k) I don't know

33	How often do you provide a report on the information security status or posture of the organisation to the following positions - Board, CEO, Senior execs?	a) Monthly b) Quarterly c) Semi-annually d) Annually e) Adhoc f) I don't know g) Never

SECTION 7 INFORMATION SECURITY RISK MANAGEMENT

34	Does your organisation have a documented and approved risk methodology?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

35	Is there a documented risk treatment plan that identifies actions, resources and funding, as well as responsibilities and priorities for managing information security risks?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

36	Does the organisation have an up-to-date risk register that specifies information security related risks?	a) Up-to-date risk register that specify information security related risks b) Risk register that specifies information security related risks but is not updated c) Up-to-date risk register but does not specify information security related risks d) Risk register exist but is not updated nor specify information security related risks e) No risk register

37	Is the risk treatment process able to define which security controls will be implemented to mitigate the identified risk?	a) Yes b) No c) I don't know

38	Has an information security training and awareness programme been documented, approved and implemented?	a) Documented, approved and b) Documented, approved, not implemented c) Documented, not approved, not d) Intended to have one documented, approved and implemented e) No f) I don't know

SECTION 8 ORGANISATIONS VIEW OF ISO/IEC 27001

39	Is someone in the organisation aware of the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC)	a) Yes b) No c) I don't know

40	Is someone in the organisation aware aware of ISO standards available such as ISO 9001, ISO 31000 and ISO 14001?	a) Yes b) No c) I don't know

41	Which other management systems has the organisation implemented? Select all that apply.	a) ISO 9001 b) ISO 14001 c) OHSAS 18001 d) ISO 20000-1 e) ITIL f) Cobit g) ISO 31000 h) ISO 27005 i) Other

42	From an information security perspective, is someone in the organisation aware aware of the ISO/IEC 27001 standard?	a) Yes b) No c) I don't know

43	What size organisation do you believe the ISO/IEC 27001 standard has been designed for and expected to be used by?	a) Small organisations (Fewer than 200 employees) b) Medium organisations (Fewer than 2000 employees) c) Large organisations (Larger than 2000 employees) d) All the above

44	What industry do you believe the ISO/IEC 27001 standard has been designed for and expected to be used by? Select all that apply	a) Basic Materials b) Consumer Goods and Service c) Financials d) Health Care e) Industrials f) Media g) Retail h) Telecommunications i) Technology and data services j) Marketing and Research k) Tourism k) Other

SECTION 9 ISO/IEC 27001 ADOPTION

45	What was the reasons for adopting the standard?	a) Mandated by a customer b) Requirement when tendering c) To gain competitive advantage d) Competitors had already achieved certification e) Because it was recognised as the best practice standard f) To ensure legal and regulatory compliance g) Other h) Standard not adopted
46	Was senior management support obtained with the decision to adopt / not adopt the standard?	a) Yes b) No c) I don't know
47	If the decision was made to adopt the standard, was a business case developed and approved?	a) Developed and approved b) Developed but not approved c) Intended to have one developed and approved d) No e) I don't know
48	Does the business case for the adoption of the standard include the certification of the ISMS?	a) Yes b) No c) I don't know
49	Is there evidence that management provide commitment to the ISMS, such as establishing an Information Security policy and objectives and communicating the importance of meeting these objectives to the organization?	a) Yes b) No c) I don't know

50	Does the organisation have a documented and approved ISMS Scope?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

51	Does the organisation have a documented and approved Statement Of Applicability (SOA)?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

52	Does the organisation have a documented and approved Document Control framework/methodology?	a) Documented and approved b) Documented but not approved c) Intended to have one documented and approved d) No e) I don't know

53	In order to comply with ISO/IEC 27001, several mandatory documents and records are required that an organisation needs to develop and provide evidence of if the organisation is pursuing certification. Is the organisation aware of the mandatory documents required when implementing the standard?	a) Yes b) No c) I don't know

54	How often is the organisations review process for ISMS documentation?	a) Bi-Annually b) Annually c) Documents get reviewed once massive changes occur in the organisation d) I don't know

55	What was the main challenges to adopt ISO/IEC 27001?	a) Maintaining the ISMS b) Understanding the standard c) Resources d) Senior management buy-in e) Cultural change within the organisation f) Other

56	What was the ISMS implementation timescale?	a) < 6 months b) 6 - 12 months c) 12 - 18 months d) 18 - 24 months e) > 24 months

57	Who was used primarily to implement the ISMS?	a) External resources (Consultants) b) Internal resources

Appendix B – In-Person Questionnaire

SECTION 1	INFORMATION SECURITY GOVERNANCE
1	What is the organisations understanding of Information Technology governance?
2	What is the organisations understanding of information Security governance?
3	What is the organisations understanding of the difference between IT governance and Information Security governance?
4	What is the organisations understanding of IT Security?
5	What is the organisations understanding of Information Security?
6	What is the organisations understanding of the difference between IT Security and Information Security?
7	Through which line of communication/committee's are the organisations board of directors and shareholders informed of information security related matters?

SECTION 2	COMPLIANCE AND FRAMEWORKS
8	What international information security frameworks and standards are the organisation aware of that provides guidance for information security within the organisation?
9	Which of these frameworks and standards was selected for consideration for the organisation to adopt and why?
10	How is the organisation enforcing as well as measuring the compliance of Security controls (Policies, Standards and procedures, reports etc.) within the organisation?

SECTION 3	INFORMATION SECURITY RISK MANAGEMENT
11	What is the reporting line of identified information security risks? And how is business involved when rating the severity of the risk?
12	How is information security risk treatment options selected in the organisation?
13	How does the organisation measure the effectiveness of the security controls implemented to mitigate the risks?

SECTION 4	ORGANISATIONS VIEW OF ISO/IEC 27001
14	Has the organisation considered adopting the ISO/IEC 27001 standard?
15	What is the organisation's understanding of the concept of an ISMS?
16	How does the organisation understand how ISO/IEC 27001 describes its ISMS?
17	How does the organisation understand ISO/IEC 27001 Plan-Do-Check-Act (PDCA) model?

SECTION 5 ISO/IEC 27001 ADOPTION	
18	Given the drive to reduce costs what risks and issues did the organisation identify when selecting the adoption of the standard?
19	Did any of the risks cause a stop of the option to adopt the standard?
20	Who manages the ISMS whitin the organisation?
21	What other responsibilities in addition to their information security duties, does this person have to fulfil?
22	When the ISMS Scope was formulated, was there any restrictions to the scope of implmenetation?
23	If so, what is the justification to exclude business units from the scope?
24	Does the organisation understand what is involved when excluding business units from the scope when implementing an ISMS, and how it will affect certification?
25	Does the organisation understand the purpose of a Statement Of Applicability (SOA)?
26	How did the organisation select the security controls of the SOA?
27	What information security documentation does the organisation currently have in place?
28	Are these documents documented and approved by senior management?
29	How are documents such as policies, standards and procedures enforced throughout the organisation?
30	How is the compliance and effectiveness of the documents measured?
31	What is the organisations understanding of the ISMS certification process?
32	What is the organisations understanding of the ISO/IEC 27002 standard?
33	Given the drive to reduce costs what risks and issues did the organisation face when implementing the standard for certification purposes?
34	Did any of the risks cause a stop of the implementation?
35	How was these identified risks treated/mitigated?
36	Did any of the risks cause a change in strategy from senior management regarding certification?
37	If it did, what was changed in the strategy?
38	What have been the results of achieving the certification?
39	What are the main costs involved in implementing, recieving and maintaining the certification?
40	What is the perceived as well as realised benefit and value the organisation received from implementing the ISO/IEC 27001 standard?
41	What is the perceived as well as realised benefit and value the organisation received from certifying the ISO/IEC 27001 standard?
42	What are some of the operational and competitive advantages the organisation received once certified?
43	If you were to implement ISO/IEC 27001 again, would there anything that you would do differently and why?