PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA

by

NKWANA MOKATA JOHANNES

Submitted in accordance with the requirements

for the degree of

MAGISTER TECHNOLOGIAE

in the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR DORAVAL GOVENDER

FEBRUARY 2015

COPYRIGHT DECLARATION

DECLARATION

STUDENT NUMBER**: 39207234**

I, **Mokata Johannes NKWANA**, declare that this dissertation:

PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA,

is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references and that this work has not been submitted before for any other degree at any other academic institution.

____________________ 10/02/2015

SIGNATURE DATE

(MR M J NKWANA)

ACKNOWLEDGEMENTS

First and above all, I praise God, the almighty for providing me the opportunity and granting me the capability to proceed successfully. I will always remember the following words from the Bishop of Mount Zion “Keep faith; never lose hope in the God of Mount Zion”. These words encouraged me all the way long until the end of my research.

Secondly, I would like to express my sincere gratitude to my supervisor **Professor Doraval Govender** for the continuous support of my M Tech, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this dissertation. I could not have imagined having a better advisor and mentor for my M Tech study. In the beginning I thought he was a difficult supervisor. However, I have realised that he is one of the best supervisors within the University of South Africa.

My sincere thanks also goes to **Mr John Kole (Senior Lecturer)** who was always giving me courage and advices that one day I will finish this tough marathon. Thanks for not ignoring my calls and the time we have spent during those calls.

I thank **Professor A dev Minnaar** for approving my research proposal and granted me an opportunity to study M Tech with the University of South Africa.

I want to express my deep thanks to all Security Managers who participated in this study. If it was not your participation, I would not have achieved the goal and objectives of my study.

I cannot finish without thanking my family. I warmly thank and appreciate my mother **Rosina Mmachuene Nkwana,** for giving birth to me at the first place and supporting me spiritually throughout my life. I want to express my gratitude and deepest appreciation to my lovely daughter, **Makgoka,** for her understanding and being a nice girl to me. And finally, “**Mma-Makgoka” Thoriso**, without your support and encouragements, I could not have finished this work. Therefore, I can just say thanks for everything and may God give you all the best in return.

EXECUTIVE SUMMARY

The protection of security information in government departments requires the active engagement of executive management to assess emerging threats and provide strong security risk control measures. For most government departments, establishing effective protection of security information is a major initiative, given the often continuous, strategic nature of typical security efforts. This requires commitments or support from senior management and adequate resources. It necessitates the elevation of information security management to positions of authority commensurate to the required responsibilities. This has been the trend in recent years as government departments are increasingly dependent on their information assets and resources, while threats and disruptions continue to escalate in frequency and cost. It is clear from numerous recent studies that organisations that have taken the steps described in this research document and have implemented effective information security risk control measures have achieved significant results in reduced losses and improved resource management. Given the demonstrable benefits, it is surprising that there have not been greater progress in effectively managing information assets. Although regulatory compliance has been a major driver in improving the protection of security information overall, this study has also shown that nearly half of all government departments are failing to initiate meaningful compliance efforts. Failure to address the identified vulnerabilities by government departments will result in espionage, covert influencing manipulation, fraud, sabotage and corruption. Information security risk control measures include the elements required to provide senior management assurance that its direction and intent are reflected in the security posture of the organisation by utilising a structured approach to implement an information security programme. Once those elements are in place, senior management can be confident that adequate and effective protection of security information will protect, as far as possible, the department's vital information assets.

Key Terms:

Government department, Information, Information Security, Protective Security, Security.

LIST OF ABBREVIATIONS

COMSEC: Communication Security

CCTV: Closed Circuit Television

IT: Information Technology

MISS: Minimum Information Security Standards

MPSS: Minimum Physical Security Standards

SRCM: Security Risk Control Measures

SAPS: South African Police Services

SLA: Service Level Agreement

SITA: State Information Technology Agency

SSA: State Security Agency

UNISA: University of South Africa

CONFIRMATION OF LANGUAGE EDITING

I, Jack Chokwe, hereby declare that I have edited the master’s dissertation entitled: “Protection of security information within government departments in South Africa” by Mokata Johannes Nkwana. An editing certificate has been provided to confirm the professional editing and proofreading of this dissertation. See Annexure H.

04/02/2015

Date

TABLE OF CONTENTS

CHAPTER 3: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA

CHAPTER 4: DATA ANALYSIS, INTERPRETATION AND DEDUCTIONS

CHAPTER 1

GENERAL ORIENTATION

1.1. INTRODUCTION

Information, in all its different forms, has become vital strategic asset, indispensable to performing any business or providing any service. Information is the foundation upon which all systems in government departments operate in South Africa and any other country. According to Buchalter (2004:2), departments and agencies must place greater emphasis on the protection of security information that could expose the nation's critical infrastructure, military, government, and citizenry to an increased risk of attack. Departments should carefully consider the sensitivity of any information the disclosure of which could reasonably be expected to cause national security harm. According to Minimum Information Security Standards (MISS) cabinet document (1998), the state has valuable information that needs to be entrusted to people in order to get the work done. Therefore, the security and management of state information is important for government departments. Government departments are investing heavily in information security, and yet there are still data breaches occurring on a daily basis (South Africa 1998).

According to the South African Official Information Act No. 156 of 1982, Section 1(2), official information should be protected to preserve personal privacy and government interest. Different legislations, policies and security measures pertaining to information security that has been implemented in South Africa and internationally, has been studied for this research (South Africa 1982). According to Brotby (2008:7), information security is not only a technical issue, but a business and governance challenge that involves risk management, reporting and accountability. Moreover, effective security requires the active engagement of executive management to assess emerging threats and provide strong cyber security leadership. The term penned to describe executive management's engagement is corporate governance. Corporate governance consists of the set of policies and internal controls by which organisations, irrespective of size or form, are directed and managed. Information security governance is a subset of an organisation's overall governance programme.

Risk management, reporting and accountability are central features of these policies and internal controls.

According to Brotby (2008:7), information security takes the larger view that the information and the knowledge based on it must be adequately protected regardless of how it is handled, processed, transported or stored. Information security addresses the universe of risks, benefits and processes involved with all information resources. It has become clear that information must be treated with the same care and prudence as are other critical organisational resources.

The aim of this study is to evaluate the security measures that are currently used for the protection of security information by South African government departments and the identification of vulnerabilities and risks that may lead to threats.

1.2. THE RATIONALE FOR RESEARCH

On December 4, 1998, the South African Government approved the MISS document as national information security policy. The MISS was compiled as the official government policy document on information security. The document must be maintained by all government institutions that handle sensitive or classified information of the state. The MISS documents lays down minimum standard for the handling of classified information, which must be implemented by government departments (South Africa 1998).

During the past years, various presidents in the United States of America (USA) implemented different strategies for the protection of information. They all tried to establish a different approach for the protection of information. Policies and directives were formulated for the protection of information. Although several policies were formulated regarding the safeguarding and protection of security information, there are still vulnerabilities, risks and new threats emerging all the time. This problem may be resolved only if security risk assessments are conducted on a continuous basis (Buchalter 2004:1-5).

According to Schweitzer (1996:13), many security managers and system managers assume they know how to establish an information security programme. It is unfortunate that most security managers have failed to establish information security programme correctly. The following case illustrates the point:

> “the information systems vice president of a large company decided that information was at risk. A member of the information system staff, with help from others, initiated an information protection programme. After a considerable effort that lasted about two years, the company auditors reported that other staff groups and the operating units were not following the security requirements, which they regarded as a systems matter” (Schweitzer 1996:13).

Information is the only intangible asset and is the most difficult to secure. From a strategic point of view, the form of information (written, electronic, and mental) should make a little difference in security investment decision. Loss of information by government departments may results with huge impact on their service delivery. At minimum, the company should know which elements of information are critical to business success and should make carefully considered strategic decisions for protecting information. Information protection is a complex and difficult issue that cannot be dealt with in a cursory manner (Schweitzer 1996:170).

Security measures that have to be implemented for the protection of information within government institutions should generally be as extensive as the value of the information to be protected. Government institutions should know the nature and extent of the risks facing the protection of security information before implementing any security measures (Lombard 2002: 10).

On 18 November 2012, Sunday Times revealed that there were about 300 pages of leaked documents on President Zuma’s corruption case. This is revealed in more than 300 pages of explosive internal electronic mails, memorandums and minutes of meetings leaked to Sunday Times. The question is: How was this information leaked from the president’s office (Sunday Times 2012:1)? The Protection of Information Act No. 84 of 1982, Section 36 (1) provides for the protection from disclosure of certain information, prohibition of obtaining and disclosure of certain information. Any person who discloses government information for personal gain shall be guilty of an offence (South Africa1982).

According to Chikane (2013:10), most of the information the government has can be accessed by the public. Some of the government information is considered confidential and cannot be disclosed to third parties who have no rights to access it. Confidentiality in this arena builds trust and opens doors to the sharing of more confidential information (Chikane 2013:10).

1.3. RESEARCH PROBLEM

In this study, the problem is the protection of security information in government departments in South Africa. Government departments are confronted with many security breaches that occur regularly whereby computers, discs and other forms of security information containing classified or sensitive information are stolen all the time. The main purpose of stealing security information is to acquire government information for personal use. Present days' security measures give rise to the leakage of information, exploitation and espionage (Foster 2012:2).

1.4. RESEARCH QUESTIONS

In response to the research problem, the study intends to find answers to the following research questions:

- What type of security risk control measures are in existence for the protection of security information in government departments?
- What security risks are associated with the protection of security information in government departments?
- Which type of security risk control measures may be put in place for the protection of security information in government departments?

1.5. RESEARCH GOAL

The goal of this study is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the threats.

1.6. RESEARCH OBJECTIVES

To achieve the goal, the study will pursue the following objectives:

- Conduct a security survey of the existing security risk control measures used for the protection of security information in government departments;
- Assess the risks associated with the protection of security information in government departments; and
- Identify security risk control measures for the protection of security information in government departments.

1.7. KEY THEORETICAL CONCEPTS

Classified information:

According to “MISS” cabinet document, (1998), classified information refers to a sensitive information which, in the national interest, is held by, is produced in, or is under the control of the state or which concerns the state and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise (South Africa 1998).

Government departments:

Government department refers to all state institutions that provide their services in terms of Public Service regulation. These are specialised areas whereby groups of people control and make decisions for a country or state. These are referred to as areas of special expertise (Urdang 1995:153).

Information:

Information is referred to as any recorded or displayed data or knowledge or content of communication, regardless of its format**.** Information is defined as the data that has been analysed and synthesized (Van der Westhuizen, Schellnach-Kelly & Geyer 2010:10).

Information security:

According to the “MISS” cabinet document (1998), information security refers to a condition created by the conscious provision and application of documents, personnel, physical, computer and communication security measures to protect sensitive information (South Africa 1998).

Information security is also referred to as the methods, procedures, and processes necessary to prevent unauthorised disclosure, modification, or destruction of information, or the loss of proprietary rights thereto. Information security applies to all information forms: paper, microforms, photographs, transparencies, magnetic (electronic), and human memory (Schweitzer 1996:7).

Information Security Risk Assessment:

Information Security Risk Assessment (ISRA) is referred to as the business process of identifying potential threats, vulnerabilities, impact and risks to the organisation and the likelihood of their occurrence. Results can be expressed in qualitative or quantitative terms or a combination of both. Information Security Risk Assessment is one component of risk management (Layton 2007:7).

Protective Security:

According to the “MISS” cabinet document (1998), protective security is a much narrower concept than National Security, although very much a part/element of the latter. This concept deals with the provisioning and maintaining of measures to protect lives, property and information and as such could include: vetting, security investigations, guarding, document, personnel, physical and Information Technology security (South Africa, 1998).

Security:

Security is defined as the implementation of cost-effective security measures that, when taken as a whole, have the effect of reducing the probability of loss-incurring events or reducing the impact of any loss-incurring events that occurs (Rogers 2005: 105).

Security Risk Control Measures:

Security Risk Control Measures (SRCM) refer to all the security measures that must be implemented to prevent, restrict and recover security-related losses. These control measures may take the following forms: human security; technical security; security procedures; security policy; and security aids (Rogers 2005: 215).

Security survey:

Security survey may be defined as a comprehensive critical on-site inspection of current security measures that are in place in an organisation, company or business in order to identify and rectify security weaknesses or excessive security measures (Rogers 2005: 57).

Threats:

Threats may be defined as any potential event or act, deliberate or accidental that could cause impact to employees or assets (Mulder 2006:27). Furthermore, Layton (2007:7) defines threat as the potential for a threat to be exercised, either accidentally or intentionally, for the purpose of exploiting a specific vulnerability.

Vulnerability:

Vulnerability means that security measures are inadequate. For example, an asset such as cash may be exposed to a security risk like robbery. Vulnerability implies a lack of security measures in relation to security risk (Rogers 2005: 109).

1.8. OUTLINE OF THE DISSERTATION

The outline of this dissertation is organised into five chapters.

Chapter One discusses the general orientation for the study by presenting the rationale for research, research problem, research questions, research goal, research objectives and key theoretical concepts.

Chapter Two of this study is a discussion of the research methodology that includes the research approach and research design. The chapter provides a discussion of the population and sample of the study, an explanation of how the data were collected and how the data were analysed and presented. This chapter also addresses reliability and validity, limitations to the study, value of the study and ethical considerations.

Chapter Three refers to literature study on the protection of security information within government departments in South Africa. In this chapter, the researcher provides a conceptual analysis for the protection of security information within government departments. This chapter also addresses MISS, security risk assessments, information security programmes, Strategic decision making, Security risk control measures and disclosure of security information.

Chapter Four discusses how the data were collected, analysed and interpreted to draw conclusion. This chapter will also address all questions that are in the questionnaire for Security Information Managers. Tables shall be used to illustrate the research results.

Chapter Five presents the research findings and recommendations and drawn from the research results.

1.9. CONCLUSION

Information security takes the larger view that the information and the knowledge based on it must be adequately protected regardless of how it is handled, processed, transported or stored. Information security addresses the universe of risks, benefits and processes involved with all information resources. It has become clear that information must be treated with the same care and prudence as are other critical organisational resources.

CHAPTER 2

RESEARCH METHODOLOGY

2.1. INTRODUCTION

This chapter presents the research methodology used in this study, namely; the research approach, research design, population and sampling, data collection methods and instruments and analysis of the data. Five government departments were randomly selected from each province, using the random sampling technique. In addition, semi-structured interviews were conducted with sampled participants using an interview schedule that consisted of open-ended questions. A semi-structured observation was conducted using a checklist. In addition, a semi-structured documentary study was done on all relevant documents to the study using a checklist. The focus was mainly government department sites, documents pertaining to the protection of security information and Information Security Managers who dealt with the protection of security information in their respective departments. Content analysis was done using categories and themes as a technique to qualitatively analyse the data. Factors such as ethical considerations, limitations to the study, validity and reliability of information and the value of this study will also be discussed.

2.2. RESEARCH APPROACH

Qualitative research approach was used in this study because it is concerned with how the social world is interpreted, understood and experienced. Furthermore, it is based on generated data which is flexible and sensitive to the social context in which the data are obtained (Mason 1996:4).

2.3. RESEARCH DESIGN

Mistry, Minnaar, Patel and Rustin (2003:60), citing Huysamen, define a research design as the plan or blueprint according to which data are to be collected to investigate the research hypothesis or question in the most economical manner.

Accordingly, the researcher used a case study design that helped him to understand the uniqueness and the characteristics of Information Security Managers within government departments (Fouchê & Delport 2011:101-112). In designing his research, the researcher started his plan by randomly selecting government departments in each province. Secondly, he planned to conduct interviews with Information Security Managers within the selected government departments because they dealt with the protection of information within government departments. An open-ended interview schedule was developed to guide the collection of data from Information Security Managers. The aim was to conduct face-to-face interviews with Information Security Managers using this interview schedule in order to obtain information on the security measures used for the protection of security information. Permission letters to conduct the study as well as interviews were forwarded to the relevant government departments. The researcher developed an observation checklist that was used to obtain information during observations that were conducted at government registries. A documentary checklist was also developed and used to obtain information for this study. The researcher studied the protection of security information in government departments within the theoretical framework of the MISS document. The focus was to test the application of the MISS document and the Protection of Information Act, 1982 (Act no 84 of 1982) and more especially critically testing the present practices, to enhance the protection of security information within government departments.

2.4. POPULATION AND SAMPLING

Probability and non-probability sampling was used in this study. According to Strydom and Delport (2011:390), in non-probability sampling the odds of selecting a particular individual are not known because the researcher does not know the population size or the number of the population. Conversely, in probability sampling, all units of analysis have an equal chance of being selected into the study. It was important for the researcher to create the opportunity for variables to be inclusive in the study in order to avoid some imbalances. The simple random sampling technique was used to randomly select five government departments in each province out of six (6) government departments (targeted population) that fell under Justice, Crime

Prevention and Security Cluster. This was done by placing them in nine bags according to provinces and randomly selected five (5) government departments per province). Those five departments are as follows: Home Affairs, Justice and Constitutional Services, State Security Agency, Correctional Services and the South African Police Service. According to Mistry *et al* (2003:111), purposive sampling involves using experts to select samples for a specific purpose. The researcher used purposive sampling to identify and purposively interview specialists, experts and officials with experience in the protection of security information. The strategy was to interview the identified Information Security Managers systematically until a number of one hundred (100) participants was reached.

After selecting the population and the sample group, the researcher made appointments with relevant heads of government departments and arranged interviews with the sample group. The researcher undertook a fieldwork by visiting the selected government departments to conduct one-on-one interviews. Only Information Security Managers were the targeted group for this study because they managed the protection of security information in their respective departments. These Information Security Managers were interviewed in groups in order for the researcher to collect data pertaining to the protection of security information.

In terms of documentary study, the researcher accessed different sources of information in order to have a better understanding and knowledge on the protection of security information in government departments in South Africa. Documents such as policies and procedures, security manuals, security posters, departmental newsletters and strategic plan documents were requested and perused in order to check the existence of security measures applied in the protection of security information. According to Strydom and Delport (2011:376), if these documents are studied and analysed for the purpose of scientific research, the method of documentary as a data collection method will become operative. Most importantly, sources such as security policy and procedures that were found in government departments helped the researcher to obtain more information that guided the study on the protection of security information.

The researcher conducted observations in all registries at the five governments departments that were randomly selected in each province. The researcher's observations were concentrated on the following Physical Protection Systems:

- To check if classified documents that were not in use were locked in the appropriate safe storage facilities such as normal filing cabinet, reinforced filing cabinet, safe or walk-in safe and strong room;
- To check whether the doors of registry offices in which classified documents were kept were fitted with security locks;
- To determine if there was proper control over movement within the registries in which classified information was handled;
- To check whether there was identification of visitors, the issue of visitor's cards or temporary permits and the escorting of visitors;
- To check if there were appropriate registers for incoming and outgoing classified documents; and
- To check if there was effective access control to restricted areas such as cryptographic, sever room and computer centres.

All the above-mentioned Physical Protection Systems were observed in order to monitor compliance in terms of the MISS.

2.5. DATA COLLECTION METHODS AND INSTRUMENTS

The researcher used an interview schedule, documentary study checklist and observation checklist as instruments for data collection.

2.5.1. Design and development of data collection instruments

The researcher designed and developed an interview schedule for semi-structured interviews that consists of 42 open-ended questions. These questions where documented in a sequence and developed in such a way that they did not go beyond the estimated time of the interview. The researcher prepared a handful of main questions with which to begin and guided the conversation. Research questions were tested and reviewed accordingly during the pilot study with a small group of participants from the intended test population. Semi-structured interviews were conducted using this interview schedule in order to collect information from

Information Security Managers who were regarded as experts in the field of security information. During the interview, the researcher managed to probe on some of the main questions. When the responses lacked sufficient details, depth or clarity, the researcher managed to clarify the answers.

The following main questions were used to collection data:

- What type of security risk control measures are in existence for the protection of security information in government department?
- What security risks are associated with the protection of security information in government department?
- Which type of security risk control measures may be put in place for the protection of security information in government department?

The follow-up questions were asked in pursuing the implication of answers to the main questions. The researcher developed questions in a language that the respondents understood (Greef 2011: 341 – 375). The data collected through this interview schedule helped the researcher to make findings and recommendations. An observations checklist was also developed in the form of variables that assisted the researcher to obtain information on the existing Physical Protection Systems. The Physical Protection Systems such as access control to registries, registers, safes, reinforced steel cabinets, strong rooms and visitor’s cards were observed using observation checklist. Observation checklist consisted of “yes” or “no” questions and the comments column. The above-mentioned Physical Protection Systems were observed according to the MISS documents. The researcher developed a documentary checklist in the form of variables that assisted to check the existing documents such as personal documents, official documents, archival material and internal newsletters. Interview schedule is attached as Annexure A, observation checklist as Annexure B and the documentary checklist as Annexure C.

2.5.2. COLLECTION OF DATA

2.5.2.1. Interviews

Appointments for interviews were arranged in advance with the heads of government departments. Various groups of participants (information security managers) were interviewed at selected government departments using one-on-one interview method. Interview schedule was used to collect data. Only open-ended questions were asked during the interviews. A group of ten officials was sampled and interviewed in each province. These groups were interviewed continuously until the number of one hundred (100) was reached. All participants were positive, respectful and helpful in responding to the asked questions. When a question was asked by the researcher, participants responded equally since they were given an equal opportunity to do so. When the responses lacked sufficient details, depth or clarity, the researcher has managed to clarify the answer. The researcher took notes during all interviews conducted. A tape recorder was also used to record all interviews. This tape recorder assisted the researcher to remind some of the facts that he could not remember or not recorded in his notes. The interviewer used semi-structured and open-ended questions to obtain in-depth information from the respondents. Semi-structured interviews were chosen for this study because it was discursive, focused and allowed both the researcher and participants to explore much on the research topic. The collected data was also recorded in a field journal. The data were then analysed and interpreted to make findings and recommendations. Permission letters to conduct interviews at government departments are attached as Annexure D1 to D14, a copy of the informed consent letter to conduct interview as Annexure E and a letter where permission was granted and approved to conduct the study as Annexure F.

2.5.2.2. Observations

An observation checklist was developed and administered for this research. This checklist was used to collect data from all registries in government departments that were randomly selected for this study. The researcher conducted a security survey on the existing security measures used for the protection of security information at government registries by using an observation checklist. The main reason why observations were conducted at government registries was the flow of sensitive information at these areas. Most government files were handled and stored at registries. Observations assisted the researcher to determine if there was compliance by government departments with security legislations such as the MISS documents and other relevant legislations. The notes of all data collected through observations was compiled and recorded in a field journal. The data were then analysed and interpreted to make findings and recommendations.

2.5.2.3. Document Study

A documentary checklist was developed and administered for this study. This checklist was used by the researcher to collect data from various documents that were requested from selected government departments. Documentary study was done on the following documents: security policies and procedures, minutes of meetings held, internal newsletters, security manuals and posters, official documents, personal files, security plan and reports. All these sources of information were studied. Data obtained from these information sources were recorded in a field journal. According to Strydom and Delport (2011:376), if these documents are studied and analysed for the purposes of scientific research, the method of document study as a data collection method became operative. When conducting a documentary study, the main focus was on the protection of security information in government departments. Furthermore, the researcher focused on the classification of documents containing sensitive information such as official documents in order to determine if such documents were classified in terms of the MISS documents. The researcher took notes of all data found with regard to the classification system. A documentary study contributed much in this study because the data obtained assisted the researcher to make findings and recommendations.

2.5.2.4. Experience

The researcher has seventeen (17) years of experience in security services. The protection of information security in government departments was one of the researcher’s responsibilities. The researcher has the necessary knowledge and skills relevant to the research topic and research questions. Moreover, the researcher worked in government departments such as Department of Agriculture, Department of Health and Social development, Department of Economic Development and Tourism, Department of Finance and currently at the Department of Labour. He acquired too much knowledge in security management that involves the protection of security information. Therefore, the researcher has the necessary skills and knowledge on the Protection of Information Act and MISS document.

In terms of relevant training and development, the researcher is a committed worker and holds various certificates programmes, including project management, electronic communication security, advanced archives and records management, State Security Agency security manager's course, counter intelligence and information protection. With his experience in government sector, the researcher managed to gain access to various sources such as security policies and procedures, minutes of meetings held, internal newsletters, security manuals and posters, official documents, personal files, security plan and reports that were used in government departments. The information gained from these sources helped the researcher to make findings and recommendations of this study.

2.5.2.5. Literature study

Literature study was conducted using books relevant to the study, conference papers, journal articles, previous theses and dissertations, government publications, course materials, literature on internet, government policies and legislations on the protection of security information. The rationale and research questions served as guidelines in obtaining the relevant literature for the research. The literature study covered the security risks control measures implemented for the protection of security information in South Africa. There was no problem encountered by the researcher during literature study and as a result, the study was successfully completed. The information obtained during literature study helped the researcher to make findings and recommendations.

2.5.3. DATA ANALYSIS

Qualitative data analysis refers to the transformation of data into findings. This involves reducing the volume of raw information, shifting significance from trivia, identifying significant patterns and constructing a framework for communicating the essence of what the data reveal (Schurink, Fouché & De Vos 2011:397).

This study was analysed by means of collaborative inquiry. This was done through a structured listing of the researcher’s interest which involves:

- the characteristics of language as communication with regard to its content, process and as it mirrors culture in terms of the cognitive structure as well as the interactive process;
- the discovery of regularities as the identification and categorisation of elements and the establishment of their connections, and as the identification of patterns;
- the comprehension of the meaning of text or action through the discovery of themes and interpretation; and
- reflection (Tesch 1992:77).

2.5.3.1. Coding and categorising the data

According to Tesch (1992:138), the first step in the analysis process is re-arrangement or re-organisation of the data. Schurink, *et al.* (2011:423) added that the data should be broken into themes and units for data analysis by coding and categorising the data. In addition, the researcher looked at the commonalities in the themes identified in the data. The comparable themes were grouped together. However, the researcher worked with one group of themes at a time. Tesch (1992:138) emphasised that if the themes are grouped together, they can be said to be in a category. The data analysis spiral from Leedy and Ormrod (2005:151) was also adopted in this study. The data collected during interviews, literature, observation and documentary study were categorised according to the key theoretical concepts:

- Security risks;
- Security risk control measures;
- Security practices / security principles; and
- Solutions on the protection of security information.

The categorisation of data was done using a filing system by opening a file for each key theoretical concepts, and information under each category was then filed chronologically.

2.5.3.2. Reflecting on the codes and categories.

Tesch (1992:145) emphasised that the researcher must pay attention to the actual content, identify and summarise the content for each category. Furthermore, the researcher should look for commonalities in content, uniqueness in content, confusions and contradictions in content and missing information with regard to the research question or topic. Furthermore, information was compared with categories in order to identify variations and similar meanings. The data collected was scrutinised daily and similar data as well as variations were categorised together and where there was a need for information, it was easily identified, obtained and then categorised.

2.5.3.3. Identifying themes and emerging explanations

Tesch (1992:78) emphasised the discovery of regularities as the identification and categorization of elements and the establishment of connections. Furthermore, the identification of patterns was done and the emerging recurring themes and interconnections between the categories and units were identified in order to establish a direct and systematic approach when analysing the data. Data were organised into file folders and computer file. Files were then converted into appropriate text units or sentences and were analysed using a computer. The data recorded by technical media was interpreted through transcription. The cassettes or tapes were repeated several times so that the researcher could get a sense of what they contained as a whole. The researcher took his time to listen to all tapes and wrote important notes. Recorded information was converted into raw data. The raw data was then analysed and interpreted to make findings and recommendations.

2.5.3.4. Develop a storyline

Tesch (1992:141) highlighted that an organising system should be developed that will make meaningful grouping of data pieces possible. The researcher combined the following four sources from which organising system derived: the research question and sub-questions; the research instruments; concepts or categories used by other authors in previous related studies and the data themselves. According to Tesch (1992:142), if the study involves an instrument for data collection, such as a questionnaire or interview schedule, the questions often provide handy categories and that adopting concepts other researchers have developed appears to be safe.

The researcher developed an organising system and adopted other researcher's concepts because it has already being applied and was workable to those researchers. Furthermore, Tesch (1992:78) emphasised the comprehension of the meaning of text or action through the discovery of themes and through interpretation. After reflecting on the data, the researcher integrated and summarised the data. A storyline was developed that explained the themes and relationships identified in the data. The data were then interpreted into understandable meaning. The data were reduced to a small and manageable set of themes. Finally, the data were then analysed and interpreted to make findings and recommendations.

2.5.3.5. Presenting the data

The researcher used tables to categorise the themes: collection, analysis and interpretation of research data on the protection of security information within government departments in South Africa. The raw data that derived from the researcher's written notes was analysed and presented in a table form.

2.5.4. Piloting

Barker (2003:327-328) defines a pilot study as a procedure for testing and validating an instrument by administering it to a small group of participants from the intended test population. Mistry, *et al.* (2003:138) added that piloting refers to the testing of your instruments. Before the researcher commenced with fieldwork, he ensured the reliability and validity of his instrument. For the instrument experimental, the researcher tested the instrument with a target group comprising 10 Security Information Managers. In addition, the researcher arranged interviews with this target group.

In setting up these interviews, the researcher drew on respondents that match the profile of the sample, but who were not included when the sample was drawn. However, participants of pilot study were not interviewed during the main study. The researcher examined each completed interview schedule and assessed each and every aspect of it, listed the problems and identified the questions that needed refining. The researcher reviewed whether the questions produced the types of responses he wanted.

In terms of observation, the researcher has selected few government departments that were used as a pilot study. A security survey on the existing security measures used for the protection of security information was conducted using an observation checklist. Moreover, the checklist to check if it was suitable to be used for this study was evaluated. Furthermore, the researcher examined compliance with the MISS document. The documentary study was tested with a targeted group by studying the existing documents in order to check compliance with information security legislations. This assisted the researcher in determining whether the documentary study will effectively play a vital role in this study. Notably, the sample used in the pilot study was not used in the main research project. The researcher made the necessary changes to the data collection instruments before conducting the fieldwork.

2.6. VALIDITY AND RELIABILITY

2.6.1. VALIDITY

Validity refers to the truthfulness, accuracy, authenticity, genuineness and soundness (Delport & Roestenburg 2011:171-205).

The researcher ensured that the data collected through the following three measuring instruments were valid: interviews, documentary study and observation.

- Interviews were considered valid because the researcher interviewed experts (Information Security Managers who had knowledge on the protection of security information in government departments) with an interview schedule based on the research questions and purpose.
- The researcher ensured that the data collected during documentary study was valid by consulting government publications, books relevant to the study, conference papers, journal articles, previous theses and dissertations, course materials, literature on internet, government policies and legislations relevant to the research questions and purpose of the study.

- The researcher ensured that the data collected was valid by conducting observations at government registries in order to determine compliance by government departments on security legislations such as the MISS documents and other relevant legislations.

The above three measuring instruments helped the researcher to measure what was supposed to be measured.

2.6.1.1. Content validity

The researcher tested the knowledge and skills of Information Security Managers through one-on-one interview in order to validate if they were really experts. The degree of consistency on how Information Security Managers answered the questions ensured content validity. The above-mentioned three data collection instruments assisted the researcher to test the knowledge and skills of Information Security Managers. With observations, documentary study and interviews, the researcher managed to draw on the specialised knowledge and skills of Information Security Managers. The three measuring instruments helped the researcher to measure what was supposed to be measured. Validation was confirmed by means of comparing the different kinds of data collected during observations and interviews in order to determine whether they are common or related.

2.6.1.2. Face validity

The assessment was fair to all Information Security Managers because everybody was given a chance to participate in the study. A good platform was created by the researcher so that all participants were given an equal opportunity to respond to the questions asked. Participants were asked the same questions as they appear in the schedule and questions were straight to the point. Most importantly, the researcher was not biased or one-sided during interviews with participants and as a result, the research was fair to the participants.

2.6.1.3. Criterion validity

When the researcher met each group of Information Security Managers, the same principle was used to group them together. The same interview schedule was used when questions were asked of all the participants. The same observation and documentary variables were tested at all the sites (government registries). Similarly, the same method of clarity seeking questions was asked for a better understanding by the researcher.

2.6.1.4. Construct validity

The validity of the findings from the interviews was checked through personal visit to the sites and through the observations. The information obtained during interviews was valid because the researcher confirmed the availability of the security measures that were implemented during the time of the study. The researcher took the findings of the research back to the Information Security Managers being interviewed and they confirmed the findings so that the researcher could be sure that they are valid. According to Delport and Roestenburg (2011:17), construct validity implies that all of the items in the measurement instrument measured the same contrast and not something else. The same observation and documentary variables were tested at all the sites (government registries) and they measured what was supposed to be measured. The researcher requested the manual and electronic documents such as policies and procedures from the participants and validated the data obtained from the interviews and the data were found valid.

2.6.2. RELIABILITY

Information Security Managers were used as the target for this research because they deal with the safeguarding of information in their respective departments. The researcher depended more on Information Security Managers as the main sources of information for this study. In addition, Information Security Managers who were dependable, consistent, stable, trustworthy, predictable and faithful were identified. A semi-structured interview schedule to ensure consistency throughout the interviews was used. Most importantly, the researcher was helped by the interview schedule to produce accurate results that do not differ from interview to interview. This means that the same criteria for questions were used for all the Information Security Managers.

However, the researcher did not lead the Information Security Managers (participants) to answer in a specific manner, thus not leading them to a specific direction. The manner in which participants responded to the research questions without hiding information, showed that they were reliable. There was consistency in responding to the questions. The researcher ensured consistency when relevant data was collected during observations and documentary study. Data collected during observations and documentary study was reliable because it assisted the researcher to make findings and recommendations.

2.7. LIMITATIONS

The researcher managed to conduct his research successfully. However, he encountered a problem that was resolved amicably with Information Security Managers in the Department of Justice and Constitutional Development. With his experience in the government sector, the researcher managed to gain access to various sources such as security policies and procedures, minutes of meetings held, internal newsletters, security manuals and posters, official documents, personal files, security plan and reports that were used in government departments. The information gained from these sources was used to guide the research questions. However, permission letters to conduct interviews were produced to the heads of government departments. Some of Information Security Managers were concerned about the confidentiality of the information obtained by the researcher. Government departments such as Department of Justice and Constitutional Development had sensitive areas where they kept secret files (court files) and were concerned about the safety of their information. After a lengthy discussion with Information Security Managers on the safety of information of such departments, the researcher managed to gain access to their sensitive areas and interviews were conducted successfully.

2.8. VALUE OF THE STUDY

This study is of paramount importance because it has value to government departments, government officials, community and UNISA. A brief discussion of the stakeholders to benefit from this research are outlined below:

Value to government departments

The findings of this study will be significant and relevant to government departments as it will address the issue of security breaches. The study will add value to knowledge, practice, policies and it will create a roadmap for implementation of such policies and security standards. The result of this study will be a long-term benefit to government departments as beneficiaries.

Value to government officials

Personnel who handle sensitive information on their daily basis will learn how sensitive information should be handled in government departments.

Value to the community

With the identification of appropriate security risk control measures for the protection of state information, information will not get into the wrong hands for illegal activities, causing disruption to safety and stability in society. Therefore, society will benefit from a safe and secure environment.

Value to the academics

Research results will be incorporated, hopefully, into the study guides of the security management programme at the University of South Africa (UNISA) to add value in the existing body of knowledge.

2.9. ETHICAL CONSIDERATIONS

This section discusses the ethical considerations in terms of UNISA Policy on Research Ethics (2007:11). There was a good relationship between the researcher and participants throughout this study. Most importantly, participants were seen as indispensable and worthy partners in this research. The researcher showed a great respect and also protected the rights and interests of participants at every stage of the study. As one of their rights, participants were given opportunity to choose whether to participate or not. Consent on a mutual beneficial arrangement was obtained from participants. Moreover, there was no physical discomfort that emerged from this research project requiring protection from the researcher.

Respondents were thoroughly informed beforehand about the potential impact of the investigation and as a result, the respondents had the opportunity to decide if they wish to withdraw from the investigation or not. There was no respondent identified to be vulnerable that the researcher could eliminate from the study. The data collected from participants was treated as confidential. The raw data was stored in lockable steel cabinets and safe so that the access could be restricted. Information stored in the computer was protected through passwords. No unauthorised persons had access to the raw data. The raw data was analysed and interpreted to make findings and recommendations. UNISA ethical clearance certificate attached as Annexure G.

2.10. CONCLUSION

Research methodology and other relevant factors such as ethical considerations, limitations of the study, validity and reliability of the information and the value of this study were discussed in this chapter. It was important for the confidentiality of collected data to be maintained between the researcher and the participants (Information Security Managers). UNISA ethical policy was followed. All Information Security Managers who participated in this research were not forced to do so. They voluntarily participated without any arguments or negative interventions. Interviews were conducted in a professional manner that resulted with the participants being happy at the end of each interview. All interviews conducted with participants were fruitful to the researcher. The researcher achieved his goal and objective of the study through the interviews, observation and documentary study as measuring instruments.

CHAPTER 3

PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA

3.1. INTRODUCTION

There is a need for the protection of security information in government departments. Most importantly, security risk control measures should be implemented and monitored by relevant government employees. Government departments have a huge responsibility to ensure that they implement legislation that governs the protection of security information. The MISS, Security aspects such as Security Risk Assessments (SRA), Information Security Programme and Security Risk Control Measures (SRCM) will be discussed in this chapter. The security risk control measures have been identified in this study and will assist the researcher to come up with appropriate recommendations to government departments for their implementation. Where information is expected from disclosure, it implies that security control measures must be applied in full without any exemptions. Exemptions are the loopholes and eventually the downfall of most organisations including government departments. The researcher provides a theoretical framework for the protection of security information within government departments.

3.2. MINIMUM INFORMATION SECURITY STANDARDS (MISS)

On December 4, 1998, the Government of the Republic of South Africa approved the “MISS” document as national information security policy. All government departments are compelled to comply with this document. The aim of establishing this policy was to ensure that the national interest of the country is protected through counter-intelligence measures. The “MISS” was compiled as an official government policy document on information security, which must be maintained by all institutions who handle sensitive or classified material of the Republic of South Africa (South Africa 1998).

According to Schweitzer (1996:144), government departments should implement relevant standards such as “MISS” as a policy guideline. Furthermore, a policy may stipulate that one or more standards are to be published to provide procedural instruction to be followed across government departments.

The “MISS” document lays down minimum standards for the handling of classified information, which must be implemented by government department that entails classification of information. According to “MISS” Cabinet document (1998), government departments have at their disposal sensitive information that requires security measures. The degree of sensitivity determines the level of protection, which implies that information must be graded or classified accordingly. Every classification necessitates certain security measures with respect to the protection of sensitive information which will be known as classified information. Moreover, the lowest classification of information is designated as “Restricted”, which refers to the classification allocated to all information that may be used by unauthorised people to hamper activities or cause an inconvenience to the individual or government departments. Such information would be suitable for all general inquiries. The next highest classification, “Confidential”, consists of information that may be used by unauthorised persons to harm the objectives and functions of an individual and or institution. Moving up the scale again is “Secret” information. Information with this designation refers to information if disclosed inappropriately, could disrupt the objectives and functions of an institution and or State. In other words, this could cause a serious damage to government departments.

Finally, the most sensitive information is graded “Top Secret”. This refers to information that is available only to staff with a need to know and those government departments which have an appropriate authority. Information of this type, if disclosed to unauthorised people, would neutralise the objectives and functions of institutions and or State. In other words, this type of information could cause exceptionally grave damage to government departments. Government employees authorised to access documentation of Top Secret must be required to sign a “Declaration of Secrecy” in order to assure control over its content. According to the “MISS” cabinet document (1998), Declaration of Secrecy refers to an undertaking given by a person who will have, has or had access to classified information that he/she will treat such information as secret (South Africa 1998).

Government departments should take into consideration the accounting practices when classifying information. Accounting practice is defined as the system of procedures and controls that an accounting department uses to create and record business transactions. Accounting practice should ideally be extremely consistent, since there are a large number of business transactions that must be dealt with in exactly the same manner in order to produce consistently reliable financial statements. Auditors rely upon consistent accounting practice when examining a company's financial statements (Bragg (2014:1). If accounting practices is not taken into consideration when classifying information, such loopholes can create serious weaknesses in Information Security Programme. This is one of the security control measures that government departments should carefully consider. Therefore, consideration should be given to the protection of financial data about sensitive matters. Such information should not be recorded openly in journals and the ledgers along with supply items and petty cash purchases. Sensitive projects should have special accounting practices designed to minimise the risk of exposing their budgets and expenditures to employees who perform only routine accounting tasks.

According to “MISS” cabinet document (1998), access to classified information should be controlled. Access to classified information is limited to a person who has an appropriate security clearance or who is by way of exception authorised thereto by the head of the institution with due regard being paid to the need-to-know principle. In order for an employee to have a valid security clearance, there is a process of security vetting that needs to be followed. Following the literature review conducted in government departments, one can argue that this process is not done according to the “MISS” documents. The vetting of employees involves rigorous procedures that need to be followed that includes: screening, qualifications verification, background checks and in-depth vetting investigations. The screening process for personnel should start at the application stage, with the applicant completing a detailed personal history statement. This should be done before an applicant may be appointed in government departments in order to prevent the hiring of unethical applicants who may disclose confidential information that could hamper activities or inconvenience government departments (South Africa 1998).

According to “MISS” cabinet document (1998), another means of protecting sensitive or classified information is by signing a Declaration of Secrecy before an applicant is appointed or during the appointing process. These declarations are intended to create a psychological impression on employees, reinforcing the importance of protecting information to which they have been entrusted. One can argue that this process is not fully adhered to in accordance or one hundred percent 100 % in government departments. These declarations are in fact legal documents and can be used as evidence in a legal action if an employee is found to be in violation of it (South Africa 1998).

According to “MISS” cabinet document (1998), all classified secret and top secret material must be locked away in a safe or metal cabinet which is of adequate strength and equipped with a security lock. It is recommended that when classified documents are not in use, they must be stored as follows:

- “Restricted documents” must be stored in the normal filing cabinet;
- “Confidential documents” must be stored in reinforced filing cabinet;
- “Secret documents” must be stored in strongroom or reinforced filing cabinet; and lastly,
- “Top Secret documents” must be stored in strongroom, safe or walk-in safe.

One may argue that this is not happening in government departments. Sensitive documents are left unattended on the tables. It is worrying that, the implementation of “MISS” is not done fully in government departments. Heads of government departments should ensure that sensitive information is stored in appropriate or recommended storage facilities to avoid tempering, alteration and theft (South Africa 1998).

Schweitzer (1996:144) is of the view that the necessary procedures must be followed for the protection of security information. An example is a standard that requires that data processing facilities be secured. Without appropriate storage facilities, government information will be compromised and ultimately fall into wrong hands.

3.3. SECURITY RISK ASSESSMENTS

Security risk assessment is the cornerstone of an effective information security programme. Security at its very nature starts with a basic understanding of risk. Virtually every information security framework is centred on understanding the risks to government departments and managing them to an acceptable level. According to Layton (2007:3), Information Security Risk Assessment is not a stand-alone process. It is the first step in a larger business process known as Risk Management. An Information Security Risk Assessment is specific to information security, and risk management is a larger business initiative involving many different types of risk assessments and other dimensions including analysis, mitigation and et cetera.

Security Risk Assessment should have an appropriate model that is understandable in government departments. The model should be designed accurately to accommodate the requirements of government departments. In addition, Layton (2007:10) identified the following Information Security Risk Assessment Model (ISRAM) to be adopted by government departments: scope and types of assessment, threats, vulnerabilities, control level of effectiveness, likelihood, impact, risk level, recommendations, analysis and final report. The Model should be applied within government departments operations and environments to effectively lower their information security risks. In this Model, assets should be identified as part of the information security programme. Assets and their values should be utilised during the risk analysis and risk management phase to help determine the cost-benefit relationship between the value of the assets and the cost of potential controls and protection.

Jay and Hamilton (2003:260) are of the view that security measures should be based on an assessment of the risks involved in the processing of information. Security measures should include: Adopting an Information Security Policy; Taking steps to control physical security; Putting in place controls on access to information; Establishing and sustain a business continuity plan; Training a staff on security systems and procedures; Detecting and investigating security breach as and when they occur.

Layton (2007:12) established Physical Information Security Assessment as the relevant type of assessment for security information. This type of assessment can be used by government departments as it focused on the physical and environmental controls only. Furthermore, this type of assessment can be performed very quickly and has the possibility of yielding some very high-risk items. A very good example is a breakdown in physical controls that ultimately results in serious and negative consequences.

Employee Assessment must be conducted to all employees who access sensitive information within government departments. According to Morgan and Boardman (2003:150), the Information Security Officer must take reasonable steps to ensure the reliability of any employee of the organisation who has access to classified information. This is recognition that inevitably classified information will be disclosed to staff in an organisation. Such disclosure must be limited to relevant staff on a need-to-know basis, since disclosure to someone who has no need to know must be at variance with that principle. According to Morgan and Boardman (2003:151), Risk Assessment must take into account the reliability of staff and that where sensitive information is concerned, government department should employ employees who are honest.

Morgan and Boardman (2003:148) emphasised security risk assessment as a vital tool to security. Morgan and Boardman (2003:148-149) established that implementing security measures that involve technology is very costly. Government departments should ensure that they implement effective security control measures that will protect information from unauthorised access, accidental loss, destruction and the nature of data to be protected.

Furthermore, Morgan and Boardman (2003:148) pointed out that there is a temptation to assume that higher security information must be synonymous with sensitive personal information. However, it must be admitted that other types of information may also be eligible for higher security.

Morgan and Boardman (2003:150) are of the view that the security strategy of an organisation should among other things consider the balance to be struck between best practice technical developments and cost. If a technical development which is otherwise best practice is to be rejected on grounds of cost, this will need to be recorded and recognised. The relevant section of the organisation's security strategy will thus need to be based on a separate risk assessment. The strategy should consider for all personal information. If technical developments which can be considered best practice are available, government departments must accept them; or if they are to be rejected, their cost must be stated with a valid reasons.

Security Risk Assessment assisted government departments to identify information security risks or potential threats. Axelrod (2004:11) found that **t**here are two sides to security risks namely: Threats and Vulnerabilities. It is not until a threat meets a vulnerability that a security incident occurs. Threats will always be out there. Threats can be discouraged through deterrence mechanisms, such as the possibility of punishment or retaliation, or they can be avoided by not engaging in activities that are threatening. Protective and defensive measures can be installed that will inform prevention attacks or ward off an attack when it occurs. Vulnerabilities can be fixed so that an attacker penetrating defences does not penetrate and cause damage.

Northrup (2006:142) and Axelrod (2004:11) found that the most common threats come from within and outside the organisation. They add that the most common identified threats are computer threats, computer viruses, employee abuse of the network and system, financial and telephone fraud. While the above incidents comprise about 80% of the risk, other examples of risk include penetration of the system, theft of information and intellectual capital, sabotage and denial of service.

According to Axelrod (2004:11-12), threats come from both internal and external sources. A very good example is the internal sources (ex-employees) that use their opportunity because they worked in the organisation. This refers to employees who were fired, particularly those who worked night shifts and weekends. If the Security Officers have not been informed about their dismissal, they would come to the facility, pretend to have lost their identity card and, because they are known, the Security Officers on duty will allow them access to the premises. The argument is that if such employee's system access has not been terminated, he or she has free reign of the systems and can be danger to government departments. This may lead to the department not taking actions against the ex-employees as it would publicly disclose deficiencies in its controls.

Furthermore, Axelrod (2004:13) pointed out that other threats are from external sources such as the hacker, thief, virus creator and distributor, spy and cyber terrorist. From a protection point of view, the source of an attack may or may not result in a different defence. An organisation will build defences that can meet all types of attacks, but this is neither physically or economically feasible. Some middle-off-the-road approach is often taken, with everyday attacks being let down through regular methods, and with the more sophisticated and damaging attacks being addressed according to their risk and the availability of cost effective countermeasures.

According to Axelrod (2004:16), it might seem reasonable to determine the level of security through economic risk analysis, laws and regulations which reflect the risk appetites of legislators and regulators, which reflect those of their constituents. Hence, certain threats, such as identity theft, are given greater prominence in laws and regulations because of the relative influence of individual voters versus corporate lobbies. The cost of protecting against such threats may well be much higher than the benefits perceived from the corporate standpoint, or even for the society as a whole. However, the potential for very expensive and damaging actions by regulators, for example, will generally favour compliance at any cost.

Rowe (2009:92) established that the most threat to trade secret is the company's own employees because they have the motive and the opportunity that outsiders lack. Employees usually have legal access to trade secret information by virtue of their employment relationship and can use that access to misappropriate trade secret. Rowe (2009:92) suggests that employees should disclose or sign an oath of secrecy for protection of State secrets.

Prunckun (1989:24) found out that there are three major sources of threats that need to be taken into consideration by Security Managers. These threats are grouped into three levels. Level one (1) threat includes surveillance by a foreign government's security or intelligence agency or surveillance by one's own national law enforcement or intelligence organisations. Level two (2) threat includes surveillance by State or local law enforcement or intelligence unit, an organised criminal group, a foreign or domestic business competitor employing a spy for hire, a private detective acting on behalf of a party interested in your business's affairs, or other professional fact finders: for example, an investigative journalist. The last threat is level 3 threat that includes non-professional surveillance, for example, an employee, a business competitor, or another interested individual or group acting on their own for profit or revenge purposes. Furthermore, a business' threat level may change from time to time due to the dynamics of its operations. Therefore, its security needs will also be required to either escalate or abate in response to these changing conditions. (Prunckun 1989:24). Peltier, Peltier and Blackley (2005:25), and Reddick (2012:212) added that the common threats to information security are technical hardware failure, errors and omissions, deliberate software attacks, acts of human error or failure, technological obsolescence, forces of nature, deliberate acts of espionage or trespass, deliberate acts of sabotage or vandalism, fraud and theft. Reddick (2012:214) found the following threats Protection Mechanisms for information security to be effective: media backup, virus protection software, firewall protection, use of passwords, employee education, security policy, information security audits, reporting of information security violations and lastly automatic account logoff. If these threats Protection Mechanisms for information security could be effectively implemented by government departments, threats to information security will be minimised or reduced (Reddick 2012:214). According to Dhillon (2011:161), involving different vendors or intelligent agents in the organisational software results in security threats. He further stated that one problem with intelligent agent technology lies at communication level because at the end of the day, intelligent agents are integrated into a legacy software systems, in which some security mechanisms already exist. It is difficult to forecast on how the existing security mechanisms will react to the introduction of intelligent agents and whether the agents will be able to bypass these mechanisms (Dhillon 2011:161). Schweitzer (1996:168) is of the view that loose talk, paper handling and attacks on computer systems are the most information risks identified in the study conducted in 1990 on security information stored in computers. It was revealed during this study that computer security is a subset of information security and that both should be implemented together for the protection of security information in government departments.

3.4. INFORMATION SECURITY PROGRAMME

An Information Security Programme refers to the overall combination of technical, operational, procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis (Brotby 2008:72).

Government departments have a huge responsibility of implementing Information Security Programme. This could be achieved if information security could be an integral part of departmental governance and integrated into their strategies and operations. According to Brotby (2008:12), the strategy must be implemented through a comprehensive information security programme that includes well-conceived and complete policies and standards. The information security programme should cover security elements such as education and training on information security, assessments of risks and impact analysis, classification of information, development and testing of plans for continuing the business in the case of disaster or interruption of services.

It is critical for management to ensure that adequate resources are allocated to support the overall departmental Information Security Programme. In order for government departments to achieve effective information security governance, it is important to establish and maintain a framework to guide the development and maintenance of a comprehensive Information Security Programme This framework will provide the basis for the development of a cost-effective Information Security Programme that supports government departments' goals. The overall objective of security programme should be to provide assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to government departments.

Solove and Schwartz (2011:69) concurred with this view and added that government departments should appoint Information Security Managers who will enforce security programmes to protect security information. In addition, Information Security Managers should ensure that they provide the necessary training on how classified documents should be stored for effective protection. They should enforce the implementation of “MISS” and evaluate its effectiveness within government departments.

Bennett (1992:111) emphasised that appropriate Information Security Programme should be implemented against unauthorised access, alteration, disclosure, destruction of information and against accidental loss.

Gutwirth, Leenes, De Hert and Poullet (2012:220) highlighted that government departments should use audit trails to control access to sensitive information. Audit trails will allow logs to be kept and be used later during investigations. Furthermore, government departments should use confidentiality enhancing technology and protection against breaches, for example, through the use of patches and encryption devices.

Goodbody (2003:22) recommended the following security measures for the protection of security information against unauthorised access, alteration, disclosure or destruction:

- Ensuring that files containing sensitive information are stored in lockable steel filing cabinets;
- Ensuring that files holding sensitive information are stored in a secure area accessible only by relevant personnel;
- Ensuring that electronic files are password controlled;
- Ensuring that access to that part of the business premises which houses personal information is password or card controlled;
- Ensuring that where computer screens (including laptops) are located in public areas (such as waiting rooms, showrooms), measures are taken to ensure that personal information is not inadvertently disclosed to members of the public;
- Drawing up an Information Handling Policy which is brought to the attention of all employees responsible for handling personal information; and
- Ensure that all staff has been adequately trained to respect and protect the confidentiality of personal information and are aware of the security standards which have been adopted”.

Bennett (1992:98) highlighted the following principles to be relevant for information security:

- Information should be regarded as held for a specific purpose and not to be used, without appropriate authorisation for other purpose;
- Access to information should be confined to those authorised to have it for the purpose for which it was supplied;
- The amount of information collected and held should be the minimum necessary for the achievement of a specific purpose;
- The level of security to be achieved by a system should be specific in advance by the user and should include precautions against the deliberate abuse or misuse of information; and lastly
- A monitoring system should be provided to facilitate the detection of any violation of the security system.

Reddick (2012:210) established that information security controls can be classified into three categories namely: Technical Controls, Operational Controls and Management Controls. Technical Controls include products and processes such as firewalls, antivirus software, intrusion detection software and encryption. These controls mainly focus on protecting the organisation's information technology and the information stored in these systems. Operational controls are the enforcement mechanisms for correcting deficiencies that various threats could exploit, backup systems, physical access controls and protection from environmental hazards. Management controls are usage policies, employees training and business continuity planning, which focuses on information security's non-technical areas. Although these are important to know, technology alone cannot solve information security problems because information security is not just a technical problem; it is a social and organisational issue as well.

In the New York context, Peltier *et al* (2005:1) pointed out that the purpose of information protection is to protect an organisation's valuable resources, such as information, hardware, and software. Government departments will meet their business objectives and mission if appropriate information security measures are selected and implemented accordingly. Therefore, government departments need to protect the information essential to the successful operation of their business.

Northrup (2006:142) pointed out that if information security is to be effective, it is critical that everyone in the organisation takes ownership of the task. It becomes everyone’s responsibility to ensure that information is protected and not just the task of a control group or security managers.

Le Veque (2006:113) added that information security exists to support organisation-wide goals, and that is subject to overall management controls to ensure the protection of security information. Information Security Managers have priorities and resources assigned to support the overall organisational mission. Information Security Managers should know which information must be protected, to what level of protection is required and the mechanisms of protecting sensitive information.

3.5. STRATEGIC DECISION MAKING

According to Brotby (2008:17), executive management has a huge responsibility that must be undertaken at various levels of government departments to ensure the achievement of effective protection of security information. Implementing effective strategic information security objectives requires leadership and on-going support from executive management. It is accepted that management has an explicit obligation to ensure adequate protection of security information within government departments. As a result, management must consider that the requirements of a multitude of legal and regulatory rules and legal standards of due care increasingly require executive management focus and commitment, oversight, impetus and resources. Without support from executive management, Information Security Managers would not effectively protect government information.

Top management should ensure that confidential information is managed properly within government departments. Olsen (2010:91) pointed out that all confidential information should be prominently denoted as such. He adds that hard copies of documents, drawings, diagrams, and the sort shall be marked as confidential or proprietary trade secrets on each page. He further states that items which are stored electronically should also openly carry appropriate designation.

Prunckun (1989:48) specified that confidential information should have a finite life span. It must be realised that despite the best-engineered security plan and the installation of the most sophisticated countermeasure equipment, eventually information which is being guarded will become known to others. He goes on to suggest that the best way to keep information confidential is to store them in one's head and not communicate them to anyone.

Morgan and Boardman (2003:107) are of the view that where information is confidential, it may not be disclosed outside the organisation and may not be used, even within the organisation, for a purpose other than that for which it was intended when obtained unless the individual has given consent to this, or the use is required by law, or is in the public interest (which is likely to be interpreted restrictively and be limited to, for example, the prevention of crime or immediate threats to health of others). In practice, it is likely that organisations handling confidential information will need to obtain an individual's consent if they wish to use the information for non-core purposes.

In the Canadian context, Knight, Chilcott and McNaught (2012:180), the organisations shall make their employees aware of the importance of maintaining the confidentiality of personal information. Care shall be used in the disposal or destruction of personal information to prevent unauthorised parties from gaining access to the information (Knight, Chilott and McNaught 2012:180). Though this study was done elsewhere, it is also applicable in the South African context that according to "MISS" cabinet document (1998), signing a declaration of secrecy is of paramount importance for the protection of sensitive or classified information (South Africa 1998).

Top management should ensure that their employees are groomed in order to capacitate them with appropriate knowledge especially of the protection of security information within government departments. According to Layton (2007:7), information security awareness, education and training are overarching principles that must be implemented in every government department. There is a clear difference between awareness, education and training. Awareness is typically directed to all users and tends to focus their attention on global security principles. Conversely, training is much more in-depth and the message is directed at a specific group or audience with an expected outcome. Education is another step beyond training where concepts and topics are covered in depth for the purpose of developing new skills and altering the outcome in some way. Education answers the question "why" and focuses on theory and research. Education is understood to continue over a period of time to master the concepts and theories.

Northrup (2006:133) discovered that accountability relative to information starts at top management who needs to understand security issues and move past the perception that it is a technical problem. He goes on to suggest that top management should develop information security awareness programmes that will make employees security conscious. Awareness is the first step towards accountability and making information security a component of internal controls and corporate governance. Government departments need to have a plan for making sure that all the right people understand their individual roles with respect to security. Senior management has to develop and create accountability and awareness by establishing specific guidelines, procedures, and policies that should be applied throughout the organisation.

Olsen (2010:91) found that employees are unaware of what constitute intellectual property and that is why they cannot protect it. Therefore, he recommends that all staff must be sensitised to the nature of trade secrets and proprietary information through effective training that must take place on a regular basis.

Goodbody (2003:93) emphasised that government departments should arrange appropriate training for all staff involved in the processing of information and ensure that staff members understand the consequences of failure to adhere to information security regulations.

Raggad (210:17) ascertained that security training programmes are made available to employees in accordance with the security requirements of their position. There are a number of factors that could lead executive management to achieve more or have effective protection of security information in government departments. In addition, Brotby (2008:58) identified the following critical factors that could assist government departments to achieve their goals with regards to the protection of security information: There was awareness that a good information security programme took time to evolve. The corporate information security function reports to senior management and was responsible for executing the information security programme. Management and staff had a common understanding of information security importance, requirements, vulnerabilities and threats, and understood and accepted their own security responsibilities. Third-party evaluation of information security policy and architecture was concluded periodically. Brotby (2008:58) also discovered that the information security function has the means and ability to administer security, especially to detect records and analyse significance, and report and act on security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.

Brotby (2008:58) identified that clearly defined roles and responsibilities for risk management ownership and management accountability are in place. A policy is established to define risk limits and risk tolerance. Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist. The reality checks of the information security strategy were conducted by the third party to increase objectivity and were repeated at appropriate times. Critical infrastructure components are identified and continuously monitored.

Brotby (2008:58) identified that service level agreement (SLA) was used to raise awareness of and increase co-operation with suppliers relative to security and continuity needs. Policy enforcement was considered and decided on at the time of policy development. A confirmation process was in place to measure awareness. Applications are secured well before they are deployed. Information control policies are aligned with the overall strategic plans. Management endorses and commits to the information security and control.

Lastly, Brotby (2008:58) discovered that there is a consistently applied policy development framework that guides the formulation, roll-out, understanding and compliance. There is awareness that, although insiders continue to be the primary source of most security risks, attacks by organised crime and other information-related legislation contribute to this. Senior management must provide support to ensure employees perform their duties in an ethical and secure manner. Management should lead by example and ensure that there is compliance on information security policies.

3.6. SECURITY RISK CONTROL MEASURES

Security Risk Control Measures refers to all the security measures that must be implemented to prevent, restrict and recover security-related losses. These control measures may take the following forms: human security; technical security; security procedures; security policy; and security aids (Rogers 2005: 215).

Tucker (1992:87) emphasised that sensitive information must be stored in a safe storage facility to prevent loss, unauthorised and misuse of information. This may include the use of encryption keys, message authentication codes and other devices that assist in maintaining the protection of security information. Of course, appropriate physical security measures must be taken to protect government information.

Raggad (2010:18) identified passwords and digital certificates as security risk control measures for the protection of information stored in computers. Information security is the protection of information resources against unauthorised access. Conceptual resources such as programs, data and information can be secured by requiring users to supply passwords and digital certificates. While passwords prove that a correct code has been entered, we are still unsure who the supposed user is, or in fact, the real person who entered the password. We can obviously employ digital certificates and biometric techniques to authenticate the user and control access to information resources but security can still be compromised because many other violations such as eavesdropping can take place. Furthermore, users who have been authenticated and admitted into the system may be dangerous. Those users may in fact, once admitted inside, initiate unauthorised activities or even intentionally perform malicious actions that could compromise the security of the system.

Brotby (2008:13) found the following security risk control measures to be appropriate for the protection of security information in government departments: physical and environmental security measures, background checks, user identification, passwords, smart cards, biometrics and intrusion detection system such as firewalls. These security risk control measures are necessary and should address both threats and vulnerabilities in a manner that reduces potential impact to a defined, accepted level.

With regards to protection principle, in the Canadian context, Knight *et al* (2012:179) discovered that personal information is protected by security measures appropriate to the sensitivity of the information. The security risk control measures shall protect sensitive or classified information against loss or theft, as well as unauthorised access, disclosure, copying, use or modification. Government departments should protect sensitive information regardless of the format in which it is held. Furthermore, the nature of the protection will vary depending on the sensitivity of the information that has been collected, the amount, distribution, format of the information and the method of storage. More sensitive information should be protected by a higher level of protection (Knight, Chilott and McNaught 2012:179).

Solove and Schwartz (2011:56) discovered that in the Department of Health, Education and Welfare, the protection of security information is of paramount importance. Furthermore, personal information is treated as secret. Personal information is protected from unauthorised people unless consent is obtained from the owner (employee). Personal information should be prevented from misuse by unauthorised people.

Edwards and Brown (2009:232) established that it is difficult for government departments to protect sensitive information. There are still information security deniers within government departments who do not want to cooperate with security requirements or security risk control measures. Furthermore, for government departments to succeed in protecting security information, they should ensure that they destroy redundant documents containing sensitive information as prescribed in the “MISS”. Moreover, all employees should sign confidentiality agreements. Employees handling sensitive information in government departments should consider that the protection of security information is a key component of their jobs. Security breaches should be prevented at all times. Employees should ensure that such security breaches are reported to the Security Manager. Key individuals should be designated to investigate reports of security breaches and incident response.

Access control in government departments is of paramount importance. Schweitzer (1996:181) defined access control as control of physical entry to a facility or object. Furthermore, access control to sensitive information required three-step process such as authorisation, identification, and authentication. Access control may refer to the approval required for an authorised person to pass information to another authorised person. For electronic form of information, control of access to information is accomplished through computer account management and the setting of controls on accounts or files. Such controls might provide for any of a number of options, such as world read, general access, private access, and authorisation list.

Layton (2007:74) stated that access control should be done to prevent unauthorised entry to valuable information and that organisations should monitor access to operating system, network services and information systems.

Prunckun (1989:29) and Olsen (2010:92) established that access to business' offices should be limited to employees and visitors who are known or have appointments. Although many organisations need a free flow of personnel and information throughout their facilities, those areas that contain the most sensitive information, documents and systems need greater protection. All other visitors should be carefully screened and their identities verified prior to entry. Access to offices should be on a restricted basis and need-to-be-there basis. If a business visitor or staff traffic is heavy, a system of custom-designed identity cards worn on employee's outer clothing can be an effective method of quickly establishing colleagues. Toilets and other isolated places should be checked at the end of the day's business for possible intruders hiding in the building.

Communication Systems within government departments need to be protected for interception. Olsen (2010:97), Quigley (2005:202) and Prunckun (1989:36) realised that e-mail or other electronic communication of confidential information should be encrypted to prevent unauthorised reading of such information. Encryption units offer an extremely high degree of security and are being able to randomly select from encryption codes. An example of these is when an agent was successful in intercepting and recording a scrambled message. Such an agent would need the services of a mainframe computer and perhaps months, or even years, of around-the-clock computing time in order to decipher the message. Facilities to do these are realistically only available to intelligence agencies of wealthy nations, and it would be a course of action not embarked upon unless the benefits are more important than the cost.

Olsen (2010:97) added that encryption technology can prevent someone from reading your organisation’s communication of confidential information or documents.

Rosenberg and Mateos (2011:218) revealed that keeping communication secret is the heart of security. He indicated that the science of keeping messages secret is called “cryptography”. The key used in cryptography is almost unique because like door locks, there is no absolute certainty that two keys are unique. But the chances of two keys being the same are limited. However, it is not easy for an employee to open another colleague’s lock if a cryptography key is used to lock the office door.

Olsen (2010:92) pointed out that Security Screening and Background Checks should be used as security risk control measures in government departments to ensure that appointed officials are security competent. Background investigations must be conducted on all employees who have access to sensitive information. Furthermore, employment history and educational history should be verified on all employees.

Furthermore, Olsen (2010:92) found out that temporary employees are given access to sensitive information without signing confidential agreements. As a result, he suggests that background checks should be conducted on them.

Raggad (2010:17) pointed out that screening and background checks of candidates have to be conducted very thoroughly to make sure that candidates with a history of poor behaviour cannot infiltrate into the system. The stringency of the security clearance associated with a position depends on the sensitivity of information accessible to this position.

In the Canadian context, Knight *et al* (2012:158) emphasised that sensitive information should be protected by a higher level of protection and that the methods of protection of security information should include physical security risk control measures such as locked filing cabinets and restricted access to offices. Secondly, organisational measures, for example, security clearances and limiting access on a “need-to-know” basis. Lastly, technological measures, for example, the use of passwords and encryption (Knight, Chilott and McNaught 2012:158). Though this study was done elsewhere, it is also applicable in the South African context in that the same physical security risk control measures should be implemented in terms of the MISS document (South Africa 1998).

Bennett (1992:110) is of the view that government information should be protected by reasonable security protection against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. The following security risk control measures were highlighted: Physical security measures (for example, locked doors and ID cards): organisational security measures (for example, clearances for access) and informational security measures (for example, encryption).

Solove and Schwartz (2011:56) supported this view and added that any organisation creating, maintaining, using or disseminating records of identified personal data must assure the reliability of the data for their intended use and must take reasonable security risk control measures to prevent misuse of the data.

Government information needs to be stored in the recommended secure storage facilities. Tucker (1992:87) indicated that storage facility is very important for the storage of classified documents or sensitive information. Government employees must ensure that security measures which are appropriate for the storage of classified information are taken to prevent loss, unauthorised access, use, modification or disclosure or other misuse of information. In addition, where an employee is required to pass on the information to a third person, then all reasonable measures must be taken to prevent unauthorised use or disclosure of that information. This may include the use of strong rooms, encryption keys, message authentication codes and other devices which assist in maintaining the logical security of computerised data.

Prunckun (1989:37) found that a business' first line of defence against penetration by a professional espionage agent is its external barriers, that is, its doors and windows. Its second line of defence is the containers that house its confidential documents, for example, filing cabinets, index drawers, and microfiche vaults. Therefore, it is essential that businesses identify all documents and records that may be the target of a professional agent and secure these in containers that minimise the risk of their acquisition by unauthorised persons.

Northrup (2006:141) argued that there is no such thing as a hundred percent (l00%) secure system. Hundred percent (100%) security is an illusion because to err is human. In any advanced security system the human factor is considered to be the weakest link. However, it is that security can be tightened and made more secure in order to provide greater assurance against the potential vulnerability resulting from conducting business in the age of information.

3.7. DISCLOSURE OF SECURITY INFORMATION

According to "MISS" cabinet document (1998), signing a Declaration of Secrecy is of paramount importance for the protection of sensitive or classified information (South Africa 1998).Therefore, it is a requirement in government departments that, applicants should sign a Declaration of Secrecy before their appointment process. The argument is that this process was not done one hundred percent (100%) in government departments. It was found in the reviewed literature that most of government employees did not sign Declaration of Secrecy (South Africa 1998).

According to Layton (2007:86), all employees should sign non-disclosure or confidential agreements for the protection of security information in government departments. This control measure is used for personnel security. In the past, many organisations have overlooked the need to extend their information security policies to business and contractual agreements. This is becoming more of a common practice and in some cases required because of the legal and regulatory requirements placed on the organisations. These declarations are in fact legal documents and can be used as evidence in a legal action if an employee is found to be in violation of.

Tucker (1992:3) added that no employees were allowed to disclose information to unauthorised persons. The only time when information could be disclosed was when it was demanded by law. Information Security Managers should ensure that information is protected at all times to prevent it against loss, destruction, unauthorised use, access, modification and disclosure of security information.

Olsen (2010:92) found that confidentiality agreement is one of the most effective tools in raising employees' awareness and sensitive information plays an important role in an organisation. If employees execute confidential agreements upon hiring and at least once a year, this will make them realise that protection of information is very important.

Raggad (2010:17) also established that all employees who are involved in security matters and those who need access to sensitive information have to sign non-disclosure agreements appropriate to their positions or prior to granting access to that information.

Solove and Schwartz (2011:55) are of the view that disclosure of security information was prohibited according to the Protection of Information Act. Furthermore, the South African courts also had their responsibility to protect sensitive information by applying information security measures for the protection of security information. Court documents were sealed and information was not disclosed to the public.

In the Canadian context, Knight *et al* (2012:158) supported the statement that government departments may enter into agreements or arrangements with their employees. This will assist government departments in maintaining confidential information without being disclosed to unauthorised people (Knight, Chilott and McNaught 2012:158).

Solove and Schwartz (2011:56) stated that for security information, government departments must establish appropriate administrative, technical and physical protection to ensure the security and confidentiality of records.

Solove and Schwartz (2011:63) recognised that disclosure of security information in government departments is of paramount importance. All employees employed by government should sign non-disclosure forms without any exceptions. This control measure should be applicable to all employees including executive management who should lead by example.

Government documents containing sensitive information should be classified in order to avoid disclosure of information to unauthorised people. Olsen (2010:89) found that once organisations have identified the trade secrets they own and where these assets reside within the organisations, they need to classify them in order of importance to the organisations mission. He added that those items that have been identified as mission critical must be afforded the utmost protection.

Olsen (2010:89) emphasised the following four classification levels to be appropriate for information security:

- *Classified*: This refers to the mission-critical information that is to be afforded the utmost *protection*. Such information is not to be disclosed to anyone outside the core group of those individuals who have been authorised to access it.
- *Confidential:* Here the access should be strictly limited to those employees who have an actual need to know.
- *Sensitive:* The information is for the use of authorised employees on a broader organisational scale. Such information should not be disclosed to unauthorized employees or outsiders.
- *Unrestricted:* such information contains public information or other information that is of little consequence to the organisation’s proprietary property.

Solove and Schwartz (2011:62) added that classification on information should be applied only to records that contained sensitive information. Furthermore, all records that were identified as sensitive should be kept as confidential. Government employees are not allowed to disclose sensitive information to any person without authorisation from the head of institution.

Olsen (2010:90) had a different view that no single classification scheme will be correct for any organisation. The needs of each government department must be considered and evaluated before any such scheme can be implemented.

3.8. CONCLUSION

There is a need to protect sensitive information in government as it poses a risk to government departments as well as the country. Thus, it can be concluded that a decisive intervention is needed in government departments to ensure that security aspects such as Security Risk Control Measures, Security Assessment and Information Security Programs are implemented in full for the protection of security information. The implementation of these aspects would ensure the smooth running of operations to inform or render a top class service within government departments. The importance and emphasis of these measures must therefore be recognised.

CHAPTER 4

DATA ANALYSIS, INTERPRETATION AND DEDUCTIONS

4.1. INTRODUCTION

In this chapter, the researcher discusses how the data were collected. Data collection was in the form of interviews, observation and documentary study. Data were subsequently analysed and interpreted to make deductions. The primary data collected for this study was from one hundred (100) Information Security Managers who work in various government departments in South Africa. An interview schedule with 42 open-ended questions was used to obtain information on the protection of security information. Interviews were recorded and transcribed to facilitate efficient coding and analysis of the collected data. Observation and documentary study were conducted in government Registry Offices. The data from the interviews, observation and documentary study were analysed for the purpose of interpretation and making deductions.

4.2. DATA MANAGEMENT AND ANALYSIS

The data for this study were collected through one-on-one interviews conducted with security experts (Information Security Managers) who deal with the protection of security information on a daily basis within government departments. All interviews were recorded using a voice recording device. In addition, a field journal was also used to record the interviews in writing. The voice recordings and field journal notes were compared and transcribed. The researcher visited Registry Offices to conduct observations and documentary studies. The visit helped the researcher to confirm what was said by the participants during the interviews. The collected data was then analysed and interpreted to make deductions. The analysed data from the interviews is presented hereunder in tables, with interpretations and deductions. Data from the observation and documentary study are qualitatively analysed and discussed with interpretations and deductions in the paragraphs that follow.

4.3. BIOGRAPHICAL INFORMATION

This section presents the analysis results on biographical information.

4.3.1. Security Information Managers (Participants)

4.3.1.1. Gender (See Annexure A question 1)

Table 4.1: Gender of Participants (N=100)

Gender of participants	Frequency	Percentage
Male	61	61.0
Female	39	39.0
Total	100	100.0

Interpretation:

This question about gender of the participants was designed to identify the representativeness of gender in terms of Information Security Managers (participants) within government departments. The majority of the respondents who participated in this study were males.

Deduction:

Male Information Security Managers are overrepresented while females are underrepresented in the security industry because previously females were not considered in the security environment. Another justification to explain the low number of females in security industry is that women and girls were overlooked. The current status of security is different. Therefore, government departments consider qualifications and gender equality. Appointments of all employees are done without discriminations. According to Mackenzie (2012:87), there is an assumption that women and girls were either victims caught up in the fray of a male-dominated conflict or were left behind by programs that likely would have benefited them in the same way they benefited male Security Officers.

4.3.1.2 Ages (See Annexure A question 2)

Table 4.2: Ages of Participants (N=100)

Age of participants	**Frequency**	**Percentage**
Younger than 25	4	4.0
26 - 35	21	21.0
36 - 45	45	45.0
Older than 46	30	30.0
Total	100	100.0

Interpretation:

The study shows that the majority of respondents who participated were between 36 to 45 years of age.

Deduction:

Previously, many people did not consider security as a career. Those who are in management now are those that took security as a career and that is why the majority of participants were between 36 - 45 years of age. It is recently whereby people started to consider security as a career and unfortunately to be an Information Security Manager, you should also have relevant experience. According to Frerks, Ypeij and König (2014:73), at the beginning of the twenty-first century , while the army finally recognised women soldiers as crucial to the military system, the new media campaign started to display pictures of female pilots, fighters or high ranking officers as the emblem of the achievements of the military reform. Today government departments have employed both men and women Security Officers in order to balance the equity.

4.3.1.3. Highest educational qualification (See Annexure A question 3)

Table 4.3. Highest educational qualification of Participants (N=100)

Educational qualification	Frequency	Percentage
High School	28	28.0
Undergraduate	32	32.0
Postgraduate	40	40.0
Total	100	100.0

Interpretation:

The study indicates that most of participants have postgraduate qualifications.

Deduction:

The reason for obtaining postgraduate qualifications is that participants want to occupy managerial positions.

4.3.1.4 Employment category (See Annexure A question 4)

Table 4.4 Employment category of Participants (N=100)

Employment category	**Frequency**	**Percentage**
Clerical	6	6
Administration	17	17
Junior Management	21	21
Middle Management	47	47
Top Management	9	9
Total	100	100.0

Interpretation:

From the data collected, most of Information Security Managers are in Middle Management.

Deduction:

Most of Information Security Managers are in Middle Management because previously security was not recognised in top management. Currently security plays a vital role in government departments that is why Information Security Managers are appointed in Middle Management and few in top management. According to “MISS” cabinet document (1998), the head of security component must have direct access to the head of the institution and seat in management meetings in order to advice management on the protection of security information as well as security functional matters (South Africa 1998).

4.3.1.5 Name of institution of participants (See Annexure A question 5)

Table 4.5 Name of institution of Participants (N=100)

Name of institution	Frequency	Percentage
State Security Agency	8	8
Department of Correctional services	12	12
Department of Home Affairs	10	10
South African Police Service	20	20
Department of Justice and Constitutional Development	12	12
Department of Labour	5	5
Department of Cooperative Governance, Human Settlement and Traditional Affairs	3	3
Special Investigating Unit	1	1
Department of Public Works	4	4
Department of Sports Arts and Culture	1	1
Department of Health	5	5
Department of Agriculture, Forestry and Fisherman	2	2
Department of Economic Development, Environment and Tourism (LEDET)	4	4
Department of Water Affairs	2	2
Department of Rural Development and Land Reform	1	1
Safety and Liaison	1	1
Department of Environmental Affairs	1	1
Department of Higher Education and Training	1	1
Social Security	1	1
Provincial Legislature	1	1
Statistics South Africa	1	1
Premier’s Office	1	1
Independent Police Investigative Directorate	1	1
Total	100	100.0

Interpretation:

The study shows that the majority of participants were from the SAPS, Department of Correctional Services, Department of Justice and Constitutional Development followed by Department of Home Affairs and State Security Agency.

Deduction:

Most participants were from SAPS because the country relies more on them as they provide the protection services. SAPS is of paramount importance. Thus, the SAPS officers should always come in a mass because should the country have less police officers. Otherwise, crime will not be reduced. Institutions such as the Department of Correctional Services as well as the Department of Justice and Constitutional Development are used to discipline or correct people who involve themselves in criminal activities; thus, their representation should always be higher than other departments.

4.4. IDENTIFICATION OF SECURITY RISKS

4.4.1. Security risk control measures existing in government departments for the protection of security information (See Annexure A question 6).

Table 4.6 The type of security risk control measures existing in government departments for the protection of security information (N=100)

What type of security risk control measures are in existence for the protection of security information in government department?	Frequency	Percentage
Technical Surveillance Counter measures (sweeping)	2	2.0
Encryption of Information Technology (IT) equipment	2	2.0
Documents containing sensitive information are classified according to the Minimum Information Security Standards (MISS)	2	2.0
Security vetting or security screening and personnel suitability check	9	9.0
Access control is done by Security Officers or Police Officers	8	8.0
Computer passwords	3	3.0
Signing of oath of secrecy/confidentiality clause or agreements or sworn in oath	2	2.0
Lockable steel cabinets, safes, strong rooms, walk in safe, reinforced steel cabinets and optimizer	15	15.0
Directives, MISS policy, Security policy, IT policy and key control policy	3	3.0
The protection of information Act, South African Police Service Act, and Criminal procedures Act	2	2.0
Registers for incoming and outgoing sensitive documents	2	2.0
Courier services for the transportation of sensitive documents	1	1.0
Information security audit or inspections	2	2.0
Biometric or electronic access control system or card readers or access cards	7	7.0
Shredder machine in place	9	9.0
Gates, electronic key pads, locks and keys	1	1.0
Documents are kept in Archives	1	1.0
Digital information is protected by pin codes	1	1.0

Documents are stored in the registry	1	1.0
Closed Circuit Television (CCTV) cameras, physical security or guarding and patrolling	2	2.0
Security awareness programme or security briefing	8	8.0
E-mails, brochures, handbooks and internal letters	1	1.0
Security Committee meetings or Risk Management Committee	2	2.0
Support from top management	1	1.0
Security points at all buildings	1	1.0
No access is allowed in the premises if an employee or visitor does not have security clearance	1	1.0
Visitors cards are implemented	1	1.0
Signing of access control register	1	1.0
Authorisation must be given before a file is given out to an official	1	1.0
Spyware	1	1.0
Information is dispatched in sealed temper proof double envelopes	4	4.0
Top secret clearance	3	3.0
Total	100	100.0

Interpretation:

The study shows that most government departments prefer using lockable steel cabinets, safes, strong rooms, walk in safe, reinforced steel cabinets and optimisers as security risk control measures for the protection of security information in government departments.

Deduction:

Lockable steel cabinets, safes, strong rooms, walk in safe, reinforced steel cabinets and optimisers are preferred by most of government departments. According to the “MISS” cabinet document (1998), this type of security risk control measures should be used by government departments to store the documents that contain classified information. Few of the respondents responded to other security risk control measures because they were the only security risk control measures implemented in their departments. It is clear that respondents could not mention the security risk control measures that are not implemented in their departments. Few participants indicated that their departments conduct security audit or inspections. It is expected from all government departments to ensure that information audits are conducted in order to monitor compliance in terms of the “MISS” document. It has been identified that few of government departments use registry to store classified documents because other government departments do not know the importance of storing classified documents in the registry. There is a clear indication that only few government departments use access control registers in order to control their access to their premises. Only few government departments adhered to the “MISS” document with regards to the classification of sensitive information because other government departments do not have knowledge on how to classify documents containing sensitive information. A very low percent of government departments use computer passwords to protect sensitive information stored in computers which becomes a high risk to government information. The main reason is that most government departments do not distinguish between non-sensitive and sensitive information. As a result, they did not have any security risk control measures to protect information stored in computers (South Africa 1998).

4.4.2. Effectiveness of security risk control measures (See Annexure A question 7).

Table 4.7 Effectiveness of security risk control measures in government departments (N=100)

Do you find the security risk control measures at your department to be effective?		
	Frequency	Percentage
Yes	57	57.0
No	43	43.0
Total	100	100.0

Interpretation:

The majority of the participants found the existing security risk control measures in their departments to be effective.

Deduction

The study shows that the identified security risk control measures are perceived to be effective because most of government departments do not know about other security risk control measures that could be used for the protection of security information. A very low percent of participants indicated that the existing security risk control measures in their departments are not effective because they are not implemented in full as required by the “MISS” document. In addition, it is because of lack of support from top management.

4.4.3. Ineffectiveness of security risk control measures (See Annexure A question 8)**.**

Table 4.8 Reason for ineffectiveness of security risk control measures (N=100)

If no, please say why you find these measures to be ineffective?	**Frequency**	**Percentage**
There is still corruption by internal staff and cannot be detected.	3	3.0
Lots of dockets are missing from the registry.	1	1.0
Identification of staff is not adequate.	1	1.0
Classification of documents is not done by all components.	2	2.0
The organisational structure is too thin.	1	1.0
Police Officers are not always in the office to handle files.	1	1.0
If there is a breakdown in security it takes a long time to fix the problem.	1	1.0
The controls might be in place but due to human factor, officials are easily tempted in giving out information regardless of controls.	1	1.0
There is non-compliance to security directives such as MISS, MPSS and security measures due to lack of support from top management.	27	27.0
Delay in vetting of officials by SSA, failure to subject officials to vetting and vetting is a once off thing and people tend to forget about it.	4	4.0
Hand metal detector is not reliable.	1	1.0
Lack of knowledge by staff and we need trained Security Officers.	2	2.0
Insufficient safes	1	1.0
Dangerous weapons are always found in possession of the public members.	1	1.0
Detectives leave the dockets unattended.	1	1.0
Wrong people can lay hands on official's access cards.	1	1.0
There is no encryption devices installed on the communication system.	1	1.0
There is no security policy in place.	18	18.0
Integrated security system is broken and left unrepaired.	4	4.0
Sharing of building create a problem when it comes to the control by security officers.	5	5.0
Insufficient fund or security budget.	12	12.0
Lack of qualified security staff.	11	11.0
Total	100	100.0

Interpretation:

Most of the respondents who participated in the study indicated that there is non-compliance to security directives such as “MISS”, “MPSS” and security measures due to lack of support from top management.

Deduction:

The reason for non-compliance to security legislations is because there is no penalty to be imposed to government departments if they fail to comply. The study also shows that few government departments operate without security policy. Consequently, the security risk control measures are ineffective. The other risk that contributes to ineffectiveness of security risk control measures in government departments is insufficient fund or security budget. Most of security risk control measures such as electronic devices are very expensive and they require more money.

4.4.4. Leakage of information (See Annexure A question 9).

Table 4.9 Leakage of information (N=100)

Indicate to what extent you agree or disagree with the following statements: **Leakage of information at Government department can be reduced if proper security risk control measures can be implemented effectively by Security Managers**		
	Frequency	**Percentage**
Strongly agree	58	58
Agree	33	33
Neutral	7	7
Disagree	2	2
Total	100	100.0

Interpretation:

One hundred (100) Information Security Managers had conflicting views about leakage of information. However, the majority strongly agreed that leakage of information may be reduced if Security Risk Control Measures could be implemented effectively by government departments.

Deduction:

There is a clear indication that Information Security Managers have positive minds, passion and are willing to have effective security risk control measures in place within their respective government departments. In addition, low percentage agreed with the above statement because it is their responsibility to ensure that the protection of security information is implemented in government departments. On the contrary, a very lower percentage of participants were neutral because they were not sure whether there is any other security risk control measures that could be implemented in their departments accept the one implemented currently. The lowest of participants disagreed with the above statement because they do not believe that there are other security risk control measures for the protection of security information that could be implemented and work better than the one they have implemented in their departments.

4.4.5. Security policies and procedures (See Annexure A question 10)**.**

Table 4.10 Availability of security policies and procedures (N=100)

Do you have security policies and procedures in place at your department pertaining to protection of security information?		
	Frequency	Percentage
Yes	78	78.0
No	22	22.0
Total	100	100.0

Interpretation:

The study shows that most government departments have security policies and procedures in place in their departments pertaining to the protection of security information.

Deduction:

The majority of the government departments have security policies and procedures in place because they want to protect government information. A very low percent of participants indicated that their departments do not have security policy because they do not see it as an important document. Security policy is the cornerstone of the institution especially when it comes to security risk control measures. According to Morgan and Boardman (2012:89), it is good practice for government departments to adopt written policies that set out principles and procedures that will ensure compliance with government legislations. In the event of any complaint or request by a data subject under the Act, the evidence that an organisation has clear written and enforced procedures for strict compliance may help to strengthen the organisation's case. Peltier, Peltier and Blackley (2005:17) added that security policy is the first and probably most important aspect of information security.

4.4.6. Familiarity with security policies and procedures (See Annexure A question 11)**.**

Table 4.11 Extent to which respondents are familiar with security policies and procedures (N=100)

How familiar are you with the security policies and procedures?		
	Frequency	Percentage
Very familiar	78	78.0
Not familiar	22	22.0
Total	100	100.0

Interpretation:

The aim of this question was to determine whether respondents were familiar with security policy and procedures currently implemented in government departments. The majority of the participants are very familiar with the policies and procedures.

Deduction:

Indeed, the majority of the participants should be familiar with the policies and procedures because they are responsible for the development and implementation of those policies and procedures. A very low percent of participants were not familiar with the policies and procedures because they were not involved in the development of such policies and procedures. In addition, some of those security policies are not yet approved or presented to all employees.

4.4.7. Access control to Registry (See Annexure A question 12)

Table 4.12 Access control to Registries (N=100)

How is access to the registry controlled in your department?	Frequency	Percentage
By electronic access control systems	32	32.0
By registry officials only	29	29.0
By a counter with burglar bars	14	14.0
Through access control registers	11	11.0
Through vetted Human Resources personnel only	2	2.0
By key custodians	3	3.0
By high security keys and locks	2	2.0
There is a surveillance camera on the passage to the registry which monitors movement of staff	2	2.0
Pre-arrangements or special request permits are completed and approved prior to access the registry	3	3.0
By in-house security officers	2	2.0
Total	100	100.0

Interpretation:

The majority of the participants indicated that access to Registries is controlled through electronic access control systems.

Deduction

Most government departments control their access to Registry through electronic access control systems because it keeps records of the people who had access on a daily basis. This system can be used to deny access to unauthorised persons. Few government departments have installed surveillance cameras to monitor the movement of staff. Most government departments did not install surveillance cameras because they are not aware that this type of security risk control measure could assist them to monitor the movement of staff who enter or leave the registry. Only few of the participants indicated that their access to the registry is controlled by key custodians. Most government departments are not aware of the importance to have a key custodian and his or her functions. Once again, access to registry in few government departments is done through vetted Human Resource personnel only because they know the protection of security information than most government departments. According to Landoll (2011:227), access control provides mechanisms that restrict access to resources to only those authorised to have access; hence, government departments should ensure that access to Registries is controlled to avoid unauthorised entry.

4.4.8. Control over outgoing and incoming documents (See Annexure A question 13)

Table 4.13.1 Outgoing register for classified documents (N=89)

Do you have outgoing register for classified documents?		
	Frequency	Percentage
Yes	73	73.0
No	16	16.0
Total	89	89.0

Interpretation:

The majority of the participants said that they control outgoing classified documents by means of a register. Eleven (11) participants did not respond to this question because they were not sure whether their departments have an outgoing register for classified documents.

Deduction:

It appears as though all outgoing documents including classified documents are recorded in a register for control purpose. A low percentage of respondents indicated that they do not have a register for outgoing documents and as a result, classified information is at risk because it is not protected or controlled appropriately as required by the “MISS” document. The lowest percentage of participants who did not respond poses a security risk because it appears that their departments do not have a register for outgoing classified documents.

Table 4.13.2 Incoming register for classified documents (N=79)

Do you have an incoming register for classified documents?		
	Frequency	Percentage
Yes	72	72.0
No	7	7.0
Total	79	79.0

Interpretation:

The majority of the Information Security Managers indicated that they have a register for incoming classified documents. However, twenty one (21) participants did not respond to this question because they were not aware if their departments have an incoming register for classified documents.

Deduction:

There is a clear indication that this register is not dedicated for classified documents only. The risk is that one register is used for both unclassified documents and classified documents. A very low percentage of participants indicated that they do not have a register for incoming classified documents and this poses a security risk on classified information that might fall under wrong hands. Twenty one percent (21%) who did not respond to the above question also poses a risk because it shows clearly that their departments do not have a register for incoming classified documents for the protection of security information.

4.4.9 Removal and dispatching of documents (See Annexure A question 14)

Table 4.14 Removal and dispatching of classified documents from premises (N=100)

How are classified documents removed or dispatched from the premises?		
Sealed security envelopes and mail bags	30	30.0
Signing of registers	20	20.0
Messenger drivers	10	10.0
Departmental vehicles	12	12.0
Courier services	11	11.0
Steel containers with high security locks	5	5.0
Written authorisation from the Director General or Head of security	4	4.0
By vetted officials	2	2.0
Removal permit	2	2.0
By hand	1	1.0
Normal envelopes	1	1.0
Electronically encrypted and password produced	1	1.0
Transported with vehicles fitted with tracking devices	1	1.0
Total	100	100.0

Interpretation:

The majority of the respondents who participated in this study pointed out that the removal and dispatching of classified documents from the premises is done through sealed security envelopes and mail bags.

Deduction:

Most respondents pointed out that the removal and dispatching of classified documents from their premises is done through sealed security envelopes and mail bags because they know that the information will be protected. The risk identified in most government departments is the removal and dispatching of classified documents by hand and the use of normal envelopes as the information will not be protected. The study further indicates that only a few percentage of government departments are using encryption devices and passwords when dispatching and removing classified documents from their premises. Moreover, most government departments that do not use encryption devices on electronic equipment that transmit classified information are at risk as their information can be intercepted at any time without being noticed or detected. According to the “MISS” cabinet document (1998), encryption devices should be used on electronic equipment that transmits classified information in order to prevent interception by unauthorised people. Furthermore, few participants indicated that classified documents are removed or dispatched by vetted officials. It becomes a risk to the departments that use officials that are not vetted because classified information may be compromised (South Africa 1998).

4.4.10. Security programmes (See Annexure A question 15)

Table 4.15 Security programmes for the protection of security information in government departments (N=100)

What security programmes are in place to make the staff security conscious with regard to protection of security information?		
	Frequency	**Percentage**
Security Awareness, education and training	61	61.0
Newsletters and circulars	32	32.0
E-mails	3	3.0
Orders	1	1.0
Inspection or Audit	3	3.0
Total	100	100.0

Interpretation:

Most Information Security Managers indicated that they have security awareness, education and training programmes in place to make the staff security conscious with regard to the protection of security information.

Deduction

The majority of government departments have security awareness, education and training programmes because they want to educate the employees and make them aware of Security Risk Control Measures for the protection of security information. It becomes a risk to few government departments that do not have this kind of security programmes as their employees are not informed about security risk control measures for the protection of security information. The study further revealed that few government departments use inspection or audit to make their employees security conscious with regard to the protection of security information of which this is not a suitable security programme for this aspect. Nevertheless, inspection could not be used to make the staff security conscious. It clearly shows that the participants who mentioned inspection or audit do not have appropriate security programmes to make their staff security conscious for the protection of security information.

Tipton and Krause (2000:200) added that in order to be successful, a security awareness programme must be implemented and it must stress how security will support the department's business objectives. All employees want to know how to get things accomplished and to whom to turn for assistance. A strong awareness programme will provide those important elements. Furthermore, all employees need to know and understand management's directives relating to the protection of security information. One of the key objectives of a security awareness programme is to ensure that all employees get this message.

4.5. ASSESSMENT OF THE RISK

4.5.1 Security risks associated with the protection of security information (See Annexure A question 16)

Table 4.16 Security risks associated with the protection of security information (N=100)

What security risks are associated with the protection of security information in government departments?	Frequency	Percentage
Theft of documents containing sensitive information	15	15.0
Theft of computers containing sensitive information	3	3.0
Leakage of information by staff members	15	15.0
Unavailability of security measures for the protection of sensitive information	1	1.0
Employee negligence with regard to office security.	2	2.0
Espionage	10	10.0
Lack of information security awareness sessions	1	1.0
Breach of confidentiality	6	6.0
Abuse of privileged information	5	5.0
Tempering with information or destruction and alteration	6	6.0
Misrepresentation of data	4	4.0
The improper removal of documents (including information in electronic format)	4	4.0
Terrorist and cyber attack	4	4.0
Disaster such as flood and fire	2	2.0
Unauthorised access to sensitive information	3	3.0
Fraud and corruption	7	7.0
Serious harm	2	2.0
Demoralised staff members	1	1.0
Throwing away documents instead of shredding them	1	1.0

Publication with the intend to discredit government	1	1.0
Transportation of classified information by couriers who are not vetted	1	1.0
Lack of communication and ignorance	1	1.0
Burglary in offices	2	2.0
Appointing foreign intelligence agent	1	1.0
Missing files	1	1.0
Employees who are not vetted	1	1.0
Computer virus	1	1.0
Total	100	100.0

Interpretation:

Most of the respondents who participated indicated that there is theft of documents containing sensitive information and the leakage of information by staff members.

Deduction

Most government employees who do not earn enough and as a result, they end up involving themselves in theft and leakage of information. Schweitzer (1996:144) is of the view that the necessary procedures must be followed for the protection of security information because without appropriate security risk control measures, government information will be compromised and ultimately be stolen or fall under the wrong hands.

4.5.2 Theft of information (See Annexure A question 17)

Table 4.17 Theft of information in government departments (N=99)

Did you ever experience theft of information in your department?		
	Frequency	Percentage
Yes	61	61.0
No	38	38.0
Total	99	99.0

Interpretation:

This question was intended to find out if there was theft of information in government departments. However, one participant did not respond to this question because he or she was not aware of any theft of information occurred in his or her department. The majority of participants indicated that they have experienced theft of information in their departments. A very low percentage of the participants responded negatively because they did not experience theft of information in their departments.

Deduction

Theft of information in government department is high because of lack of sufficient security risk control measures. If security risk control measures could be implemented in full, the rate of theft will not be high.

4.5.3 Method used by perpetrators to steal information (See Annexure A question 18)

Table 4.18 Method used to steal information in government department (N=100)

If 'yes' please indicate below how this information was stolen in your department.	**1**	**2**	**3**	**4**	**5**
Theft of computer and laptops from offices	11 (11%)	5 (5%)	2 (2%)	1 (1%)	1 (1%)
Theft of laptops from official's own vehicles	12 (12%)	4 (4%)	7 (7%)	1 (1%)	1 (1%)
Missing files from registry	2 (2%)	1 (1%)	1 (1%)	2 (2%)	3 (3%)
Burglary in office	1 (1%)	1 (1%)	1 (1%)	1 (1%)	2 (2%)
Corruption by internal employees	6 (6%)	4 (4%)	4 (4%)	4 (4%)	16 (16%)
Interception from computer/ computer hacking	3 (3%)	1 (1%)	1 (1%)	1 (1%)	1 (1%)

Interpretation:

The majority of the participants indicated that information was stolen from their department through theft of laptops and computers either from office or vehicles. However, corruption by internal employees was rated very high.

Deduction:

Laptops and computers keep more information that may be retrieved if stolen by unauthorised persons. In addition, laptops and computers are very expensive and can make more money if someone sells them at a good price. According to "MISS" cabinet document, (1998), all computer storage media that contains classified information must be handled according to the document security standards.

4.5.4 Reporting of crime (See Annexure A question 19)

Table 4.19 Establishing whether crime is reported by respondents (N=77)

Did you report any of these experienced crime or theft of information?		
	Frequency	Percentage
Yes	62	62.0
No	15	15.0
Total	77	77.0

Interpretation:

The majority of the respondents who participated in the study indicated that they have reported the crime they have experienced. Fifteen (15) participants responded negatively to this question because they were not aware whether the experienced crime or theft of information was reported or not.

Deduction

Theft of information was reported because the departments wanted to prevent classified information stolen. In addition, the main purpose of reporting crime is to ensure that the case is investigated maybe the culprit or the stolen item could be found. In table 4.19 , which displays the data on reported crime, it is clear that very few cases were not reported whereas more crime were reported to the relevant people or institutions and will be investigated by the SAPS. The fifteen percent (15%) of unrecorded crime is regarded as the “dark figure”. Therefore, the dark figure is highly concentrated at the nonserious end of the crime seriousness spectrum. What has to be stressed is that it cannot be assumed that the amounts of unrecorded crime have stayed constant throughout in government departments (Walsh and Hemmens 2011:43).

4.5.5 Institution or People to whom crime was reported (See Annexure A question 20)

Table 4.20 Institutions or People to whom crime was reported in government department (N=100)

If ‘yes’, to whom did you report these crime or theft of information?		
	Frequency	**Percentage**
State Security Agency (SSA)	14	14.0
Head of Department	16	16.0
South African Police Service (SAPS)	40	40.0
Manager or Supervisor	30	30.0
Total	100	100.0

Interpretation:

Most crimes were reported to the South African Police Service (SAPS) and Manager or Supervisor followed by Head of Department and State Security Agency.

Deduction

Employees within government departments have faith in the South African Police Service (SAPS) as well as their Managers or Supervisors. Employees believe that if crime is reported to these people or institution, actions will be done from security point of view. Employees are aware that the risk of reporting the crime to the State Security Agency, Head of Department, Managers or Supervisors is that crime might not be investigated properly as compared to the SAPS. In addition, employees are not receiving feedback from their Manager or Supervisor if crime is reported to them. Furthermore, it becomes a risk to report a crime and at the end of the day there is no case number that could be used for enquiries if crime is reported to the State Security Agency, Head of Department, Manager or Supervisor as compared to the SAPS. SAP as a government system is legally mandated to manage the policing of crime. Therefore, government departments rely more on SAPS with regards to the reporting of crime that occurred in their organisations (Ross 2000:157).

4.5.6 Action taken after crime was reported (See Annexure A question 21)

Table 4.21 Action taken after crime was reported (N=64)

Was any action taken after this incident or theft of information was reported?		
	Frequency	Percentage
Yes	57	57.0
No	7	7.0
Total	64	64.0

Interpretation:

The majority of the participants replied that action was taken after this incident or theft of information was reported**.** However, 36 participants did not respond to this question because this type of crime did not occur in their departments.

Deduction

Seven percent (7%) of participants indicated that no action was taken after theft of information was reported and this poses a high risk to government departments. The majority of the participants indicated that action was taken by relevant officials and institutions. This is presented in the next table.

4.5.7 Specific action (See Annexure A question 22)

Table 4.22 Specific action that was taken after crime was reported (N=57)

If yes specify what was done?		
	Frequency	Percentage
Investigations were conducted by State Security Agency (SSA), South African Police Services (SAPS) and internal security	47	47.0
Disciplinary measures taken	5	5.0
Criminal case opened	4	4.0
Fingerprints were taken	1	1.0
Total	57	57.0

Interpretation:

The majority of the participants indicated that investigations were conducted by SSA, SAPS and internal security. However, the participants did not respond to this question because there was no crime reported to their departments or no action was taken after theft of information was reported to their manager or supervisor and Head of Department.

Deduction

Forty three percent (43%) of the participants did not report theft of crime that took place in their department. As a result, they did not respond to the above question. It is a risk for government departments if they fail to report crime that occurs in their departments as no action will be taken against the culprit. The table above indicates clearly that the majority of government departments have reported a crime to SSA, SAPS and internal security who in return conducted investigations.

4.5.8 Security clearance certificates (See Annexure A question 23)

Table 4.23 Security clearance certificate issued to employees (N=93)

Do all personnel who handle sensitive information in your department have a valid security clearance certificates?		
	Frequency	Percentage
Yes	50	50.0
No	47	47.0
Total	97	97.0

Interpretation:

This question was aimed at checking whether the personnel handling sensitive information has valid security clearance certificates. Majority of Information Security Managers responded that personnel handling sensitive information in their departments have valid security clearance certificates**.** Three (3) participants did not respond to this question because they were not aware whether employees in their departments have a valid security clearance certificates.

Deduction

Forty seven percent (47%) of the participants responded negatively while three percent (3%) did not respond to the above question because employees in their departments are handling sensitive information without a valid security clearance certificates. In other words, information may be compromised and fall under wrong hands or unauthorised persons. Furthermore, only fifty percent (50%) of government departments have a valid security clearance certificates and this poses a high risk to government information. Most government employees will then have access to classified information while they do not have a valid security clearance certificates which offers them an authority to access and handle classified information.

4.5.9 Level of security clearance (See Annexure A question 24)

Table 4.24Level of security clearance certificate issued to employees (N=50)

If 'yes' please indicate the level of security clearance they have.		
	Frequency	Percentage
Top secret	6	6.0
Secret	4	4.0
Confidential	21	21.0
Top secret, secret and confidential	7	7.0
Secret and confidential	12	12.0
Total	50	50.0

Interpretation:

This question was asked to determine the level of security clearance certificates issued to employees. The majority of the participants indicated that employees in government departments are cleared to the level of confidential. Nevertheless, the participants did not respond to this question because their departments do not comply with the "MISS" document.

Deduction:

The table above shows that most of the employees in government departments are cleared to the level of confidentiality because they deal mostly with confidential information than secret or top secret information. However, the participants did not respond to this question because their departments do not comply with the "MISS" documents. Non-compliance to the "MISS" documents is identified as a risk to those government departments where 50 participants came from, because classified information will be compromised and handled by unauthorised people who may also leak or steal it for their personal gain.

4.5.10 Receiving of mail (See Annexure A question 25)

Table 4.25 Receiving of mail or files by employees (N=97)

How do employees receive official files within their sections?		
	Frequency	Percentage
Signing mail register	27	27.0
Security envelopes	9	9.0
Hand delivered	10	10.0
Non-security envelopes	6	6.0
Signing mail register and security envelopes	10	10
Signing mail register and hand delivered	26	26.0
Security envelopes and hand delivered	8	68.0
Signing mail register, security envelopes and hand delivered	1	1.0
Total	97	97.0

Interpretation:

This question was aimed at establishing how mail or files are received by the employees. Most of respondents who participated in the research answered that employees in their departments are signing mail register when receiving their mail. However, the participants did not respond to this question because they did not have knowledge on how employees receive their mail or official files in their department.

Deduction:

The reason for signing mail register is for control purpose and to ensure the protection of security information. This process will assist Registry personnel should there be any mail missing from their offices. A very low percentage of the participants mentioned various security risk control measures for receiving their mail and official files. However, three participants did not respond to this question because they do not have any security risk control measures in place in their departments for the receiving of mail and official files which is a high risk for the protection of security information. It is also a risk to government departments that the use of non-security envelopes for classified documents as the information is not protected. Non-security envelopes can be easily be opened by a person who deliver the mail without being noticed. In addition, mail or files containing classified information will easily be accessed by unauthorised persons if there is no proper security risk control measure in place when mail or official files are received. According to Solove and Schwartz (2011:56), any organisation disseminating records of identified personal data must assure the reliability of the data for their intended use and must take reasonable security risk control measures to prevent the misuse of the data.

4.6. SECURITY RISK CONTROL MEASURES

4.6.1 Security risk control measures for photocopying classified documents

(See Annexure A question 26)

Table 4.26 Security risk control measures for photocopying classified documents (N=99)

Are there security risk control measures in place when photocopying classified documents?		
Yes	46	46.0
No	53	53.0
Total	99	99.0

Interpretation:

The majority of the participants answered that there are no security risk control measures in place when photocopying classified documents. One (1) participant did not respond to this question because he or she was not aware of whether there was security risk control measures implemented in his or her department for the photocopying of classified documents. Forty six (46) participants indicated that they have security risk control measures in place when photocopying classified documents in their departments and will be discussed in the table that follows.

Deduction:

Most government departments fail to implement security risk control measures for photocopying classified documents because they do not know what security risk control measures to be used to protect sensitive information when photocopying classified documents.

4.6.2 Specific security risk control measures (See Annexure A question 27)

Table 4.27 Specific security risk control measures for photocopying classified documents (N=46)

If 'yes' please specify.		
	Frequency	Percentage
Photocopying register	35	35.0
Pin codes	2	2.0
Dedicated photocopy machine for classified information	3	3.0
No copies unless authorised	2	2.0
Photocopy machine is encrypted	2	2.0
Classified documents are photocopied by the documents owner	1	1.0
Photocopy machine is placed in a separate office where is not accessible by everybody	1	1.0
Total	46	46.0

Interpretation:

This question was asked to establish what security risk control measures are in place for photocopying classified documents. The majority of Information Security Managers revealed that a register for photocopying classified documents is in place. However, 54 of them did not respond to this question because they do not have any security measure implemented in their departments for photocopying classified documents. These participants were complaining about insufficient budget and lack of support from top management. In addition, security awareness programmes are not being sufficiently implemented by all government departments with regard to the security risk control measures for the photocopying classified documents.

Deduction:

The majority of the participants mentioned that a register for photocopying classified documents is in place for control purposes. Few government departments mentioned different security risk control measures however it becomes a risk to these departments that do not have any security risk control measures in place. In other words, government information will not be safe because there is no security risk control measures in almost fifty four percent of government departments as indicated by the participants for the photocopying of classified documents. According to Whitman and Mattord (2008:272), if copies of classified information are not controlled properly, classified information may be compromised or fall into wrong hands.

4.6.3 Security risk control measures for destruction of redundant documents

(See Annexure A question 28)

Table 4.28 Security risk control measures for destruction of redundant documents (N=100)

Are there security risk control measures when the destruction of redundant documents containing sensitive information is done?		
	Frequency	Percentage
Yes	46	46.0
No	54	54.0
Total	100	100.0

Interpretation:

The majority of the respondents that participated in this study replied that there is no security risk control measures when the destruction of redundant documents containing sensitive information is done. Forty six percent (46%) of the participants responded positively to this question and have managed to indicate the security risk control measures that are in place for the destruction of redundant classified documents. These security risk control measures will be discussed in the next table that follow.

Deduction:

The majority of the participants responded negatively because they do not have any security risk control measures in place for the destruction of redundant classified documents. The participants indicated that security is not recognised by top management and therefore they are unable to implement security risk control measures. In addition, the participants mentioned that employees do not attend to security awareness programmes so that they could be educated on how to protect classified information in their departments. A very low percentage, that is, 46 of the participants responded positively. However, this is not satisfactory in terms of compliance to the “MISS” document. According to “MISS” cabinet document (1998), government departments are subjected to the Archives Act, 1962, when destruction of classified documents done. Furthermore, when destruction has been properly authorised, it should take place by burning or a shredder (South Africa 1998).

4.6.4 Specific type of security risk control measures for destruction of redundant documents (See Annexure A question 29)

Table 4.29 Specific security risk control measures for destruction of redundant documents (N=46)

If ‘yes’ please specify the type of security risk control measures?		
	Frequency	Percentage
Shredding machine	31	31.0
Burning	4	4.0
Approval from the National Archives	11	11.0
Total	46	46.0

Interpretation:

This question was intended to find out about types of security risk control measures implemented for the destruction of redundant documents. The majority of the participants stated that shredding machines are used for the destruction of redundant documents followed by approval from the National Archives and burning. However, some of the respondents did not respond to this question because they did not know what type of security risk control measures were implemented in their departments for the destruction of redundant documents, or generally they did not have any security risk control measure in place.

Deduction:

It is a risk that fifty four percent (54%) of the respondents that do not have any security risk control measures in place for the destruction of redundant classified documents. If these documents are thrown away without being destroyed, information may fall under wrong hands or unauthorised persons and at the end of the day this might cause harm to government departments or affect their objectives. A very few of the participants responded positively to this question. This shows that they adhere to the "MISS" document, thus, shredding machines are used for the destruction of redundant documents in order to protect sensitive information that might be thrown away by government employees.

Whitman and Mattord (2008: 272) are of the view that if shredding machines are not used, the people who engage in dumpster diving may retrieve information and thereby compromise the protection of security information within government departments.

4.6.5 Protection of communication equipment (See Annexure A question 30)

Table 4.30 Protection of communication equipment for interception (N=46)

Are communication equipment protected for interception in your department?		
	Frequency	Percentage
Yes	36	36.0
No	62	62.0
Total	98	98.0

Interpretation:

This question was asked to determine if security control measures are in place for protection of communication equipment. The majority of the participants retorted that there are no security control measures in place for protection of communication equipment. Two (2) participants did not respond to this question because they were not aware whether communication equipment was protected for interception in their departments. Thirty six percent (36%) of the respondents responded positively because they have security risk control measures in place which will be presented in the table that follows.

Deduction:

Most participants responded negatively to this question because of lack of sufficient budget to purchase the encryption devices that could be used for the protection of the communication equipment for interception. In addition, some participants indicated that they do not know the security equipment to be used to protect their communication equipment from interception of which this becomes a high risk for those government departments that are affected by this.

Very few participants responded positively because they are trying to comply with the “MISS” document, thus, their communication equipment is protected for interception. Table 4.31 will present the security risk control measures that are implemented in order to protect communication equipment as indicated by the thirty six participants.

4.6.6 Explanation on the protection of communication equipment (See Annexure A question 31)

Table 4.31 Explanation on the protection of communication equipment for interception (N=36)

If 'yes' please explain how is it protected.		
	Frequency	Percentage
Communication equipment are protected by encryption devices	29	29.0
Firewalls, antivirus, passwords, pin codes and spyware	6	6.0
Scrambler on all telephones	1	1.0
Total	36	36.0

Interpretation:

The majority of the participants answered that communication equipment is protected by encryption devices followed by firewalls, antivirus, passwords, pin codes, spyware and scrambler on all telephones. However, 64 participants did not respond to this question because their communication equipment is not protected for interception.

Deduction:

Only thirty six (36) of the participants responded positively. This becomes a high risk to government information as it appears that most of participants responded very negatively. If communication equipment is not protected as prescribed by "MISS" document, classified information will be transmitted unsafely and might fall under unauthorised persons.

4.6.7 Storage facilities for classified documents (See Annexure A question 32)

Table 4.32 Storage facilities for classified documents N=100)

Are there safes, strong rooms or re-enforced steel cabinets for the storage of classified documents in your department?		
	Frequency	Percentage
Yes	98	98.0
No	2	2.0
Total	100	100.0

Interpretation:

The majority of the participants cited that there are safes, strong rooms and re-enforced steel cabinets in place for the storage of classified documents. Nonetheless, only a few percentage of the participants responded negatively because their departments do not have funds to purchase or install the above mentioned security risk control measures.

Deduction:

Ninety eight percent (98%) of the participants responded positively because their departments complied in terms of the “MISS” document as they are compelled to have safes, strong rooms and re-enforced steel cabinets for the storage of classified documents. It is a risk to the two percent of the departments that do not comply to the “MISS” document as this will result with their department losing classified information due to lack of security risk control measures.

4.6.8 Storage facilities in general (See Annexure A question 33)

Table 4.33 Storage facilities for classified documents (N=2)

If ‘no’ please indicate how are classified documents stored in your department?		
	Frequency	Percentage
Wooden filing cabinets	2	2.0
Total	2	2.0

Interpretation:

Two percent (2%) of the respondents who participated in the study cited that classified documents are stored in wooden filling cabinets. Ninety eight (98) participants did not respond to this question because they do not use wooden filing cabinets, instead they use safes, strong rooms and re-enforced steel cabinets for the storage of classified documents not wooden.

Deduction:

There is a clear indication that government departments who use wooden filling cabinets do not have appropriate storage facilities such as re-enforced steel cabinets, safes and strong rooms to store classified information.

4.6.9 Access control to computer room (See Annexure A question 34)

Table 4.34 Access control to computer room (N=100)

Is access to computer/sever/network room controlled?		
	Frequency	Percentage
Yes	100	100.0
Total	100	100.0

Interpretation:

This question was asked to determine if there were security measures for the control of access to computer room. All participants agreed that there are security measures in place for the control of access to computer room.

Deduction:

Access to computer room is controlled in order to prevent unauthorised entry by unauthorised persons.

4.6.10 Specific security measures for computer room (See Annexure A question 35)

Table 4.35 Specific security measures for computer room (N=98)

If 'yes' please specify how it is controlled?		
	Frequency	Percentage
By Information Technology (IT) personnel only	49	49.0
CCTV, security door and locks	5	5.0
Electronic access control system	39	39.0
Security registers	5	5.0
Total	98	98.0

Interpretation:

This question was aimed at looking specifically at the type of security measures implemented for the control of access to computer room. The majority of the participants indicated that access to computer room is controlled by Information Technology "IT" personnel only. The next highest percent of the participants indicated electronic access control. The lowest percentage of participants indicated CCTV, security door, locks and security registers. However, two (2) participants did not respond to this question because their computer room is not controlled.

Deduction:

Ninety eight percent (98%) of the participants indicated that they have security risk control measures for computer room. It becomes a risk for the two percent (2%) of government departments that do not comply to the "MISS" document with regard to the implementation of security risk control measures for computer room in order to protect government information. This may result with government information being tempered with or computer system being intercepted by unauthorised person who will have uncontrolled access to the computer room. The main risk is that if access to computer room is not controlled, every employee will have access and may temper with computer equipment or sever. According to "MISS" cabinet document (1998), access to classified information should be controlled. Access to classified information is limited to a person who has an appropriate security clearance or who is by way of exception authorised thereto by the head of the institution with due regard being paid to the need-to-know principle (South Africa 1998). Goodbody (2003:22), added that government departments should ensure that were computer screens (including laptops) are located in public areas, security measures should be taken to ensure that personal information is non inadvertently disclosed to members of the public.

4.6.11 Protection of information in computers (See Annexure A question 36)

Table 4.36 Protection of information in computers (N=100)

Do computer users protect information stored in their computers?		
	Frequency	Percentage
Yes	89	89.0
No	11	11.0
Total	100	100.0

Interpretation:

The majority of the participants confirmed that computer users protect information stored in their computers. A few percentage of the participants responded negatively that the computer users do not protect information stored in their computers.

Deduction:

Eleven percent (11%) of the participants responded negatively because their departments are not doing anything about the protection of information stored in the computers. Furthermore, those participants gave the reason that their IT section is responsible for computer equipment including the creation of passwords and installation of antivirus devices. Thus, they fail to protect information stored in the computers. It is a risk to government departments who do not have any security risk control measures to protect information stored in computers as computer hackers may have a free access to classified information. The majority of the participants indicated that the computer users protect information stored in their computers because they prevent sensitive information from unauthorised persons. Computer users know that if they fail to protect information stored in their computers, it will be compromised and that unauthorised persons will have a free access to classified information.

4.6.12 Specific protection of information stored in computers (See Annexure A question 37)

Table 4.37 Specific protection of information stored in computers (N=89)

If 'yes' please specify how computer users protect information stored in their computers?		
	Frequency	Percentage
Passwords	88	88.0
Fire walls and antivirus	1	1.1
Total	89	89.0

Interpretation:

The majority of the participants mentioned that passwords are used by computer users to protect information stored in their computers. Only one (1) participant indicated fire wall and antivirus. However, 11 participants did not respond to this question because they did not know what security risk control measures were used in their departments to protect information stored in the computers.

Deduction:

It is a risk to government information to find that only one percent (1%) of the respondents who participated in this study has indicated fire wall and antivirus. This indicates that 99% of government departments have failed to install security risk control measures such as fire wall and antivirus to protect information stored in computers. In addition, 88 participants indicated computer password because to them this is the only security risk control measure that they know could assist them in protection classified information stored in the computers.

4.6.13 Approach by outside people (See Annexure A question 38)

Table 4.38 Respondents approach by outside people (N=100)

Have you ever been approached by outside people requesting you to provide government information in exchange of money or anything?		
	Frequency	Percentage
Yes	7	7.0
No	93	93.0
Total	100	100.0

Interpretation:

The majority of the participants said that they were not approached by outside people who requested information in exchange of money. A few percentage responded positively to this question and their explanations will be discussed in the table that follows.

Deduction:

Seven percent (7%) of the participants responded positively because outside people wanted to corrupt them. In addition, ninety three percent (93%) of the respondents responded negatively because they were not approached by any outside people as they are afraid to be arrested or convicted of fraud or corruption. According to Silverstone and Sheetz (2007:81), fraud is perpetrated against companies by outsiders and this has caused million in losses. Furthermore, the government departments are in real risk if they fail to implement an appropriate security risk control measures because the impact of fraud may result with million losses of government information.

4.6.14. Explanation on the approach by outside people (See Annexure A question 39)

Table 4.39 Explanation on the approach by outside people (N=100)

If 'yes' please explain how were you approached by outside people requesting you to provide government information in exchange of money or anything?		
	Frequency	Percentage
Respondents were approached by outsiders to steal files or dockets in exchange of money.	2	2.0
Respondents were requested to alter information from SAPS dockets or departmental tender documents.	4	4.0
Respondent was promised a vehicle in exchange of secret files.	1	1.0
Total	7	7.0

Interpretation:

The majority of the participants cited that they were approached by outside people who requested them to alter information from SAPS dockets or departmental tender documents. Few of the participants indicated that they were requested to alter information from SAPS dockets or departmental tender documents. Only one (1) participant indicated that he was promised a vehicle in exchange of secret files. Nonetheless, ninety three percent (93%) participants did not respond to this question because they were not approached by outside people requesting information from them in exchange of money.

Deduction:

Ninety three (93) participants did not respond as they were not approached by the outside people because they are afraid to be arrested of stealing government information. Four (4) of the participants indicated that they were requested to alter information from SAPS dockets or departmental tender documents in order to win the tender or their cases. One (1) participant indicated that he was promised a vehicle in exchange of secret files because she wanted to cause harm to government officials who were involved in the awarding of tender for the rendering of cleaning services.

According to Oosthuizen, Shapiro and Strauss (1983:54), “the free exchange of information and ideas is being seen in South Africa as a threat to those sectional interests that have become our legislature’s primary concern, and consequently, the news media have been subjected to the sweeping restraints and are additionally required to operate under constant government threats of increased censorship”.

4.6.15 Solutions on the protection of security information in government departments (See Annexure A question 40)

Table 4.40Types of security risk control measures (N=100)

Which types of security risk control measures may be put in place for the protection of security information in government departments?	Frequency	Percentage
Regular security awareness	1	1.0
Vetting of employees to the level of top secret	10	10.0
Restriction of access to sensitive areas	1	1.0
Network security such as firewalls, password and antivirus	1	1.0
Information security audit	2	2.0
Physical security for file	1	1.0
Classification system for securing information	9	9.0
Proper storage of information	6	6.0
Proper dispatching of information and documents	6	6.0
Proper destruction of information	5	5.0
Signing of oath of secrecy	1	1.0
Effective access control	2	2.0
Policy on network devices	1	1.0
Installation on encryption devices	1	1.0

Employee training on information security	1	1.0
Shredding of documents that are unused	1	1.0
Security awareness must be conducted on a monthly basis	7	7.0
Vigilance by Security Officers in terms of searching during access control at gates must be enforced more seriously	1	1.0
Implementation of integrated security system (CCTV, access control and fire warning)	2	2.0
High security locking system	1	1.0
Effective access control system such as x-ray machine	1	1.0
Appointment of information security officers	1	1.0
All physical security measures	1	1.0
Access to classified information must be denied to authorise people	1	1.0
South African police officers must be disciplined at all times	1	1.0
Prioritize critical areas such as vetting of personnel	1	1.0
Backup system away from business premises	1	1.0
I-pad must be handled the way computers are handled	1	1.0
Burglar doors and burglar proofs must be installed in all offices	1	1.0
Upgrade security clearance of police officers to the level of top secret	1	1.0
All security measures recommended in the miss documents such as steel cabinets, strong room, safes and vetting of personnel	1	1.0
Finger prints /dump security (Biometrics system)	2	2.0
Encourage staff members to attend security awareness programme	1	1.0
Top management should support security system	1	1.0
Strengthen the control of access to information and	1	1.0

communication technology equipment		
Protection of server room	1	1.0
Burning the use of USB	1	1.0
Searching upon entry and exit	1	1.0
Proper register for sensitive information (in & out going registers)	1	1.0
Circular	1	1.0
Proper registry control measures	1	1.0
Disciplinary measures must be taken against employees who conduct security breaches	1	1.0
Appointment of key custodian	1	1.0
Purchasing of safes and re-enforced steel cabinets	1	1.0
Appointment of information security managers	1	1.0
All files should be locked away when not in use	1	1.0
Photocopying machines cleared on knock off time	1	1.0
Laptops must always be locked by the locking cables	1	1.0
Bags with seals used by the messengers	1	1.0
Ad-hoc scanning of memory sticks and external hard drives	1	1.0
Proper filing system that will allow SAPS to secure information	1	1.0
Stop out-sourcing security services to private security company	1	1.0
State Information Technology Agency (SITA) must invest in new security measures to protect information	1	1.0
Total	100	100.0

Interpretation:

This question was asked to determine what type of security risk control measures may be put in place for the protection of security information. The majority of the participants proposed that vetting of employees should be upgraded to the level of top secret. The next highest percent of the participants indicated the classification system for security information followed by security awareness that must be conducted on a monthly basis. A very low percentage of participants indicated other different types of security risk control measures that may be put in place for the protection of security information such as signing of oath of secrecy, installation of encryption devices, protection of server room and other security risk control measures as indicated on the above table.

Deduction:

The majority of the participants emphasised that the vetting of employees should be upgraded to the level of top secret because they have realised that confidential clearance certificate lasted for a long period and employees may end up doing corruption and resign without being noticed. Confidential clearance lasts for a period of twenty (20) years of which this becomes a high risk to government information because an employee will join the department being clean knowing that he or she will not be detected if involved in any criminal activities for that period. According to the “MISS” document, top secret clearance is reviewed every five years. Furthermore, the study revealed that sensitive information is not classified according to the “MISS” document because of lack of knowledge by government employees. The study further revealed that there is a lack of security awareness in government departments with regard to the protection of security information due to lack of support from top management. Generally speaking, security risk control measures that are mentioned in the above table are still not enough to protect classified information in government departments. A very low percentage of the participants indicated signing of an oath of secrecy, installation of encryption devices and protection of server room of which this becomes a risk to other government departments that do know have knowledge with regard to the mentioned security risk control measures.

4.6.16 Improvement of security measures (See Annexure A question 41)

Table 4.41 General improvement of security (N=100)

In your opinion, what should be done to improve the protection of security information in general in your departments?	Frequency	Percentage
Encourage all employees to comply with the MISS policy and procedures	6	6.0
Encourage support from top management	6	6.0
Laptops must be encrypted	7	7.0
Improve security structure by appointing information security practitioners	1	1.0
Testing of security measures	1	1.0
Information security must be developed, monitored and implementation of MISS document	7	7.0
Replace manual assets management system with electronic system	6	6.0
Information session or awareness to staff on regular basis	10	10.0
Regular security checks	1	1.0
Police station should ensure that information is treated accordingly and be protected	1	1.0
Access should be denied on high job profile	1	1.0
Effective security system at all restricted areas	1	1.0
Security vetting, more vigorous vetting and screening	7	7.0
More steel cabinets	1	1.0
SITA and COMSEC to improve IT security and communication security system	1	1.0
People dealing with classified information should be aware and familiar with the classification system and filing system	1	1.0
Sharing of computers must be stopped	1	1.0
Implement whistle blowing	1	1.0
Password must be changed every week or monthly basis	1	1.0
Appointment of security managers	1	1.0
Training of staff	7	7.0
Allocation of resources (Budget and manpower)	1	1.0

Effective counter measures to fight fraud and corruption	1	1.0
Penalties for employees who remove classified information without authorisation and those who leave classified information on their tables without locking them away after work	1	2.0
All staff members must sign oath of secrecy	1	1.0
Install fire walls and antivirus protection	1	1.0
Search vehicles	1	1.0
Implement encryption devices on electronic communication devices	1	1.0
Establish security committee that will address security issues especially information security	2	2.0
Reporting of irregularities/corruption activities especially on information security	1	1.0
Security guards must be posted at restricted areas	1	1.0
Visit by National Security officers (intelligence) yearly	1	1.0
To make the executive management informed about protection of classified information	1	1.0
Request funds to procure security measures like encryption devices, biometric devices to control access to offices	1	1.0
Fire alarm system, fire detectors must be installed at registry offices	1	1.0
Proper access control measures	1	1.0
Police must work with community to improve their work rate	1	1.0
Awareness should be escalated to contractors as well	1	1.0
All personnel must be vetted to the level of top secret clearance	1	1.0
Classification of documents	1	1.0
Top management must approve security policy	1	1.0
Cancel all memory stick on computers	1	1.0

There must be an appropriate storage of movable devices such as CD, DVD and USB (memory sticks)	1	1.0
Security management should be prioritised in government department as it plays a vital role	1	1.0
Decisive intervention is needed in the legislative and framework governing information	1	1.0
All those who will fail the vetting process should not be allowed to work with confidential information	1	1.0
Integrated security control measures must be put in place	1	1.0
Documents must be locked behind locked doors	1	1.0
Secure transportation of information in sealed envelopes	1	1.0
Encourage whistle blowing policy or people to report wrong-doing by internal staff	1	1.0
Total	100	100.0

Interpretation:

This question was asked to determine what should be done to improve security risk control measures in government departments for the protection of security information. The majority of the participants suggested that information session or awareness should be conducted to staff on regular basis. Different opinions were raised about what should be done to improve the protection of security information in general in government departments. Seven percent (7%) proposed security risk control measures such as security vetting, more vigorous vetting and screening, laptops must be encrypted, implementation of “MISS” document and training of staff. A very low percentage suggested the following security risk control measures: improve security structure by appointing information security practitioners; police station should ensure that information is treated accordingly and be protected; effective security system at all restricted areas; more steel cabinets, allocation of resources (budget and manpower); penalties for employees who remove classified information without authorization and those who leave classified information on their table without locking them away after work and lastly; request funds to procure security measures like encryption devices, biometric devices to control access to office.

Deduction:

The study indicates clearly that participants are prepared to protect classified information by educating employees through information session or awareness and training however they receive the necessary support from top management. The participants are also eager to comply with the “MISS” document; hence, they proposed that employee be encouraged to comply with the “MISS” policy and procedures. The study further indicates that only a few percentage of the participants mentioned other different security risk control measures that should be implemented in government departments for the protection of security information. However, it becomes a risk as not all government departments are willing to implement the identified security risk control measures indicated on the above table. It appears from the study that government departments are not ready to use common information security standards for the protection of security information.

4.6.17 Changing of security risk control measures (See Annexure A question 42)

Table 4.42 Changing of security risk control measures for effectiveness (N=100)

What security risk control measures do you think need to be changed in YOUR department to make them more effective for the protection of security information?	Frequency	Percent
The department must consider changing card readers with biometrics access control system	2	2.0
Restriction to classified information needs to be intensified by management	11	11.0
Policies and procedures	3	3.0
Access to the department – all people moving in and out of the department must be regulated	1	1.0
Access to registry must be through biometrics systems	1	1.0
Vetting and pre-employment screening must be prioritised	15	15.0

to employees who have access to classified information.		
There must be penalties for employees who leave classified information on their tables without being locked away	1	1.0
Uncontrolled photocopying of classified information	1	1.0
The use of electronic filing system instead of manual	1	1.0
Employ security staff/personnel who are qualified or who have relevant qualification, knowledge and skills	1	1.0
Restriction to classified information need to be intensified by management	1	1.0
Access to buildings and sensitive areas	1	1.0
Registers used at registry	2	2.0
Security forum must be held monthly instead of quarterly	2	2.0
Upgrade security clearance level to top secret clearance only	1	1.0
Improved on the storage facilities for classified documents	1	1.0
Install biometric access control system and CCTV to all buildings	4	4.0
Delivery of submission in security envelopes	2	2.0
To concentrate on training of personnel with regard to the handling and storage of classified documents	1	1.0
Using vetted officials from private security companies before employing them	1	1.0
There should be a permanent employee who irresponsible for the protection of information in all SAPS police stations who does not work shifts	1	1.0
Provide valid security clearance certificate	1	1.0
Safes containing case files must be locked during the night and be opened during the day only	1	1.0
Sharing of passwords	3	3.0
Do not throw away unused documents	1	1.0
Access control	1	1.0

The department must stop employing wrong personnel on security posts as they do not have experience	1	1.0
No cellular phones or I-pad should be allowed in sensitive meetings	1	1.0
Security officers must be placed or posted to control access to the boardroom where classified information is discussed	1	1.0
Sweeping of boardrooms where classified or sensitive information is going to be discussed	1	1.0
Vetting should be done in-house and not by SSA as it takes years to obtain feedback	1	1.0
Compulsory security training.	1	1.0
Effective security awareness.	3	3.0
Effective security committee supported by top management	1	1.0
Bags with seals need to be checked by security and the registers when documents are taken out of department by messengers	1	1.0
Installation of optimiser instead of wooden drawers	1	1.0
Privatisation of government security services as it leads to corruption	2	2.0
All sensitive documents must be classified and be stored according to its sensitivity	1	1.0
Building keys must be controlled by security only	1	1.0
Making use of re-enforced steel cabinets	1	1.0
Free access to all government buildings need to be changed	1	1.0
Vetting of police officers from confidential to top secret clearance	1	1.0
A docket must be scanned and kept safe electronically with back-up system	2	2.0
Computer rooms must be controlled by one responsible person in order to safe guard the department information	1	1.0

Department should stop employing people before conducting background checks	3	3.0
To ensure that registry develop registers for classified documents	2	2.0
To ensure that only registry personnel with clearance are allowed to work in the registry	1	1.0
Educate all staff on how to classify sensitive documents	1	1.0
Provide lockable storage facilities in the department	1	1.0
Searching should be done by technological equipment and not manual	1	1.0
Proper use of communication security and encryption system	1	1.0
Actions to be taken against negligent losses of laptops containing sensitive information	1	1.0
Only people with necessary security clearance must be given access to classified documents	1	1.0
Appointment of more security staff	1	1.0
The use of hand metal detector must be changed to walk-through metal detector	1	1.0
Changing of four or three lever locking system to a cylinder locks	1	1.0
Attitude by officials towards security must be changed	2	2.0
Total	100	100.0

Interpretation:

This question was asked to determine what security risk control measures need to be changed in order to make them more effective in government departments for the protection of security information. The majority of the participants indicated that vetting and pre-employment screening must be prioritised to employees who have access to classified information. The next higher percentage of the participants indicated restriction to classified information needs to be intensified by management. The table above indicates various security risk control measures which the participants want them to be changed in order to make them more effective for the protection of security information: the department must consider changing card readers with biometric access control; access to the registry must be done through biometric system; uncontrolled photocopying of classified information; the use of electronic filing system instead of manual; registers used at the registry; delivery of submission in security envelopes; making use of reinforced steel cabinets and other security risk control measures as indicated in the above table. Participants further emphasised that departments should provide lockable storage facilities, proper use of communication security and encryption devices, the use of hand metal detector must be changed to walk-through metal detector and lastly, changing of four or three lever locking system to a cylinder locks.

Deduction:

The majority of the participants indicated that vetting and pre-employment screening must be prioritised to employees who have access to classified information because it is a risk for government departments who employed applicants without the application of these security risk control measures. Pre-screening of applicants is of paramount importance because it eliminates employees who have illicit activities when they apply for employment in government departments especially when it comes to handling of classified information. The study shows that there is free access to classified information by government employees; hence, the participants indicated restriction to classified information needs to be intensified by management. There are a number of proposed security risk control measures that need to be changed in government departments. As a result, this shows that classified information is currently at risk with ineffective security risk control measures implemented in government departments.

According to Carrol (1977:104), a contrast exists between vetting as it can be done by private firms and government agencies. A private firm is able to inquire into personal habits that go to establish reliability, whereas such inquiries are often forbidden in government departments.

4.7. OBSERVATION.

Observations (See Annexure B) were conducted by the researcher at various government departments. The main target was Registry Offices because it is where the flow of information takes place. It was observed that all one hundred percent (100%) of government departments have security measures in place for the protection of security information. However, there is no uniformity. Most of security measures implemented for the protection of security information is vetting of personnel. Access to classified information is controlled. However, different security measures were used. The most security risk control measures used to control access to classified documents were electronic access control systems. It was confirmed during observation that most of the government departments, (98%) indeed have safes, strong rooms, reinforced steel cabinets for the storage of sensitive information. Only two percent (2%) of government departments uses wooden filling cabinets. It was discovered that doors or filing systems are fitted with security locks and that combination locks are used in most of the departments. In terms of transportation, normal government vehicles are used to transport unclassified and classified documents. It was observed that in most instances, receipts were signed by the addressee and returned to sender when classified documents were delivered. It was also observed that registers for photocopying and destruction of classified documents and unclassified documents were used. There were few security alarms implemented at the Registry Offices to monitor the movement of personnel entering and leaving the area. Most government departments have key control policies in place. All officials sign for their office keys.

Interpretation:

Observation reveals that most government departments have security risk control measures for the protection of security information. However, there is no uniformity. It was established that different security risk control measures were used in various departments for the protection of security information. However, the most one was vetting of personnel.

Deduction:

Government departments implement different security risk control measures because they fail to comply with the "MISS" document that contains common security standards for the protection of security information.

4.8. DOCUMENTARY STUDY

Documentary study (see Annexure C) was conducted in one hundred (100) government departments where one-on-one interviews were conducted with participants. During the documentary study, it was discovered that seventy two percent (72%) of security policies were in place however thirty percent (30%) of them were not approved. All of those security policies cover the protection of security information. Eighty percent (80%) of government departments have files for security clearance certificates for employees who handle classified documents. The study revealed that only fifty nine percent (59%) of government departments have security manuals and posters. In addition, seventy three percent (73%) of government departments have security registers to record classified documents. Records of security meeting such as minutes, attendance registers and agendas were kept in all government departments. Security legislation such as the Protection of Information Act has been utilised in most of government departments. All employees' personal files are classified as confidential. Documents containing sensitive information are kept in the Registry Offices for control purpose. It was discovered during the documentary study that most employees keep other file including classified files in their offices instead of sending them to Registry. Seventy one percent (71%) of government departments have kept records of confidentiality agreements or oath of secrecy. However, it was established during the documentary study that fifty percent (50%) of government departments did not classify documents that contains sensitive information.

Interpretation:

Most of employees keep files including classified information in their offices instead of keeping them at the Registry Office. Furthermore, most of documents that contain sensitive information are not classified according to their level of classifications.

Deduction:

Employees keep classified documents in their offices instead of sending them to Registry because they wanted to access information on daily basis without delay or following Registry processes. Furthermore, most documents that contain sensitive information were not classified according to their level of classification because employees do not know how to classify such information.

4.9. CONCLUSION

The collected information was descriptively analysed. Data from the interviews, observation and documentary study data were analysed, interpreted and deductions made according to the research objectives. All conclusions drawn from the research results will be discussed as findings with recommendations in the next chapter.

CHAPTER 5

FINDINGS AND RECOMMENDATIONS

5.1. INTRODUCTION

This study was conducted because government departments are faced with many security breaches that occur regularly whereby laptops and documents containing classified or sensitive information are stolen. Furthermore, the leakage of information, exploitation and espionage are also great challenges within government departments. The purpose of this study was to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information and to recommend appropriate security risk control measures to mitigate the threats. The data collected through interviews, observation and documentary study was analysed and interpreted in Chapter 4. The researcher managed to achieve the goal and objectives of the study supported with his experience in the public sector. This chapter presents the findings and recommendations based on the analysis of the collected research data.

5.2. RESEARCH OVERVIEW

The protection of security information in government departments is governed by the "MISS" document. According to "MISS" cabinet document (1998), sensitive or classified information must be exempted from disclosure and must enjoy protection against compromise (South Africa 1998).

The "MISS" document sets out the fundamental responsibilities and security programmes for Information Security Managers in government departments. It is a directive or guideline that outlines the foundation, implementation and effective monitoring of security risk control measures in government departments. It also gives the Information Security Managers the authority to take the necessary actions in security breaches that relates to the protection of security information on behalf of the Head of the Department. There is an absolute need for effective security risk control measures to be implemented in order to counter espionage, the leakage of information, the theft of information, corruption and unauthorised disclosure of information. This study was intended to determine if there is compliance with the “MISS” document by government departments in South Africa. In order to achieve the study objectives, the researcher conducted interviews, observation and documentary study.

5.3. FINDINGS

The biographical information provided by the participants in the study showed that the majority of Information Security Managers were males as compared to females. It was further established that majority of respondents who participated were between 36 – 45 years of age. In terms of highest qualifications obtained, most of the participants have postgraduate qualifications. The researcher made the following findings and recommendations in accordance with the objectives of the study.

5.3.1 PRIMARY FINDINGS

5.3.1.1 Poor dispatch of classified documents

It was found that most of government departments remove and dispatch their classified documents by hand, using normal envelopes (non-security envelopes).

5.3.1.2 Lack of surveillance cameras (CCTV)

It was found that the majority ninety five percent (95%) of government departments did not install surveillance cameras because they are not aware that the type of security risk control measure could assist them to monitor the movement of employees who enter or leave the Registry.

5.3.1.3 Poor control over the destruction of redundant documents containing classified information

It was found that the majority fifty four percent (54%) of government departments did not have security risk control measures when the destruction of redundant documents containing sensitive information takes place.

5.3.1.4 Classified information is communicated through unprotected communication equipment

It was found that the majority sixty two percent (62%) of the government departments did not have security risk control measures in place for the protection of communication equipment that are used to communicate classified information. Observations revealed that most government departments did not install encryption devices on communication equipment to protect classified information because of insufficient security budget and lack of knowledge with regard to this type of devices.

5.3.1.5 Most of employees have confidential clearance that gives them an access to classified information for a long period without being renewed

It was found that confidential clearance lasts for a period of 20 years without being renewed. As a result, this poses a security risk to government information because most of employees may use this as an opportunity to commit crime.

5.3.1.1.6 Employees handle classified information without valid security clearance or pre-employment screening

It was found that the employees handle classified information without valid security clearance or pre-employment screening. The current security weakness is the handling sensitive information without a valid security clearance certificates makes security clearance a risk in government departments and it is found to be high. It is likely that employees may use the opportunity of not having a valid security clearance to do corruption, leak information or steal classified information knowing that there is no security risk control measure in place. The impact is found to be serious. It is likely that government departments may lose classified information due to employees who do not have valid security clearance. Employees may do too much corruption knowing that government departments do not have security risk control measure that will detect their corrupt activities. It was found that most employees are not security vetted or screened during their employment in government departments. Nevertheless, they have access to classified information.

5.3.1.7 None-compliance of “MISS” document

It was found that the majority twenty seven percent (27%) of government departments do not comply with the “MISS” document with regard to the protection of security information. The study revealed that only a few government departments adhered to the “MISS” document with regards to the classification of sensitive information. It is worrying that the majority of government departments do not have knowledge on how to classify documents containing sensitive information.

5.3.1.8 Failure to distinguish between non-sensitive and sensitive information

It was found that the majority of government departments do not distinguish between non-sensitive information and sensitive information. Consequently, they did not have any security risk control measures to protect information stored in computers.

5.3.1.9 Unapproved security policy and procedures

It was found that the majority seventy eight percent (78%) of government departments were operating with draft security policies and procedures; hence, their security risk control measures for the protection of security information were not effective.

5.3.1.10 Poor classification system

It was found that most documents that contain sensitive information were not classified according to their level of classifications because employees do not know how to classify such information. The study revealed that sensitive information is not classified according to the “MISS” document because of lack of knowledge by most of government employees.

5.3.1.11 Lack of security risk control measures for photocopying classified documents

It was found that most of the government departments do not have security risk control measures in place when photocopying classified documents.

5.3.1.12 Leakage of information

It was found that the majority fifty eight percent (58%) of employees leak classified information due to lack of security risk control measures for the protection of security information in government departments. Lack of security risk control measures creates an opportunity to employees to leak classified information. Should the information be leaked by an employee, the impact will affect the objectives or functions of the department as the leakage might cause harm. The probability (likelihood) for leakage of information by staff is found to be high as there are no security risk control measures in place to prevent the employees from leaking the information. The impact is found to be very serious should classified information be leaked out of government departments. In other words, classified information may fall under the wrong hands or unauthorised persons who may in return use it for their own benefit in order to disrupt the main objectives of government departments.

5.3.1.13 Opportunity to commit theft

It was found that most the government departments have experienced theft of documents containing sensitive information. The study revealed that theft of information in government department is high because of lack of sufficient security risk control measures. The opportunity to commit theft is very likely in government departments due to lack of sufficient security risk control measures. The probability (likelihood) to get an opportunity to commit theft by internal staff is found to be high due to lack of security risk control measures. Should the employees get an opportunity to steal classified information, the impact will be very serious because unauthorised persons may cause harm or disrupt the objectives of government departments by using the information to discredit government departments.

.

5.3.1.14. Lack of network security (firewalls, antivirus, pin codes and spyware)

It was found that the majority sixty two percent (62%) of government departments do not have their computer equipment protected by firewalls, antivirus, pin codes, and spyware. The study revealed that most of employees still lack knowledge with regard to this type of security risk control measures.

5.3.1.15. Lack of security awareness

It was found that there is a lack of security awareness in government departments with regard to the protection of security information due to lack of support from top management.

5.3.2. SECONDARY FINDINGS

5.3.2.1. Lack of training

It was found that most of the government departments do not have knowledge on how to classify documents containing sensitive information. The study revealed that there is lack of training with regard to the classification of documents that contain sensitive information. Nonetheless, most government departments did not install surveillance cameras because they are not aware that this type of security risk control measure could assist them to monitor the movement of staff who enter or leave the Registry. This is because of a lack of training from government departments.

5.3.2.2. Poor management

It was found that the majority twenty seven percent (27%) of government departments do not comply with security directives such as “MISS”, “MPSS” and security measures due to lack of support from top management. It was further found that most of the government departments do not have restriction to classified information as this need to be intensified by management.

5.3.2.3. Insufficient security budget

It was found that the major risk that contributes to ineffectiveness of security risk control measures in government departments is insufficient fund or security budget. Most of security risk control measures such as electronic devices were not installed in government departments to control access to classified documents because of cost.

5.4. RECOMMENDATIONS

It is suggested that the following recommendations be implemented in government departments for the protection of security information in South Africa:

5.4.1 Poor dispatch of classified documents

Government departments should ensure that the following security risk control measures are implemented when classified documents are dispatched from premises: sealed security envelopes; steel containers with high security locks, signing of outgoing classified register; appropriate transportation services such as courier services; removal permit and dispatch must be done by trustworthy persons (employees who have valid security clearance certificates).

5.4.2 Lack of surveillance cameras

Government departments should ensure that surveillance cameras are installed in order to monitor the movement of people who enter or leave the Registry.

5.4.3 Poor control over the destruction of redundant document containing classified information

Appropriate security risk control measures such as a shredding machine, burning and approval from the National Archives must be implemented by government departments in order to control the destruction of redundant documents containing classified information.

5.4.4 Classified information is communicated through unprotected communication equipment

All communication equipment such as fax machines, laptops, computers, radio systems and telephone networks that are used to transmit or convey sensitive information to be encrypted by encryption devices for the protection of security information. These units offer an extremely high degree of security. Furthermore, government departments must ensure that when dealing with protected disclosures and in order to ensure confidentiality, the telephone line (which is also used as a confidential fax) must be separated from the switchboard. E-mails must also be monitored by the Information Technology (IT) Unit.

5.4.5 Most employees have confidential clearance that gives them access to classified information for a long period without being renewed

Vetting of employees should be upgraded to the level of top secret as confidential clearance last for a long period and employees may be involved in illicit activities without being detected.

5.4.6 Employees handle classified information without valid security clearance or pre–employment screening

Government departments should ensure that pre-employment screening is conducted to all applicants before employment or during appointment process. Pre-employment screening should be carried out to prevent hiring unethical people who may disclose confidential information. Security vetting and pre-employment screenings are the most important processes to ensure the protection of security information. Security vetting and pre-employment screening can be regarded as the first line of defence that government departments have to protect its information. Pre-employment screening is required when a person is first employed, promoted, transferred or performs general official duties in a post that will give him or her access to classified information. Most importantly, this security risk control measure is necessary because people change over time. Implementation of security vetting by government departments will assist government departments from employing employees who are untrustworthy. It is further recommended that all personnel who have access to classified documents be vetted to the level of top secret clearance in order to strengthen the protection of security information in government departments. Security clearance certificate should be used as a key to access classified information. Moreover, employees who do not have valid security clearance certificates should be denied access to classified information. Security vetting and pre-employment screening must be prioritised to employees who have access to classified information as this did not happen in most of government departments.

5.4.7 None-compliance to “MISS” document

Decisive intervention is urgently needed in the legislative and regulatory framework governing the protection of security information. It is recommended that administrative document such as the “MISS” be complied with by all Information Security Managers in order to have effective protection of security information in government departments. Subsequent to this, departmental security policies must be developed in line with the “MISS” so that there are common standards on the protection of security information applied in all government departments. In addition, Information Security Managers should ensure that they play a vital role in developing, implementing or enforcing and monitoring of information security policies so that they become more familiar with the security policies and procedures.

5.4.8 Failure to distinguish between sensitive and non-sensitive information

Government departments should ensure that they implement appropriate security risk control measures such as computer passwords and encryption devices to protect information stored in computers. Furthermore, government departments should intensify training of employees on the protection of security information that will enable employees to distinguish between sensitive and non-sensitive information.

5.4.9 Unapproved security policy and procedures

All government departments should ensure that they develop clear security policies and procedures that cover the protection of security information. Security policies and procedures must be approved as these are the cornerstones of the institution. There should be a clear directive that lay down procedures with regard to the handling of information that requires protection against leakage or disclosure of classified information. Most importantly, top management should support Information Security Managers to enforce security policies and procedures especially on the protection of security information. Information Security Managers should ensure that they familiarise themselves with the security policy and procedures as these are the cornerstones of the department.

5.4.10 Poor classification system

Documents containing sensitive information should be classified according to its degree of sensitivity. Each document should be identified with a marking indicating its classification level (rubber-stamped Confidential, Secret or Top Secret in red ink). By using an information classification system, inappropriate disclosure is likely to occur, and the protection of security information becomes effective for the department.

5.4.11 Lack of security risk control measures for photocopying classified documents

Government departments should ensure that a photocopying register is implemented when photocopying classified documents. The photocopy machine must be encrypted with encryption devices.

5.4.12 Leakage of information (Oath of secrecy or confidentiality agreements)

Government departments should ensure that employees who have access to classified information sign oath of secrecy forms or confidentiality agreements in order to protect them from leaking classified information.

5.4.13 Opportunity to commit theft

Government departments should ensure that they implement appropriate security risk control measures for the protection of security information in order to prevent employees’ opportunity to commit theft. If appropriate, security risk control measures for the protection of security information could be effectively implemented, the rate of opportunity for employees to steal classified information will be low.

5.4.14 Lack of network security (firewalls, antivirus, passwords, pin codes and spyware)

Firewalls and antivirus should be installed in computers to protect electronic data. Computer users should use passwords to protect unauthorised access to their computers. Passwords should be changed on a monthly basis in order to limit unauthorised access to sensitive information stored in their computers.

5.4.15 Lack of security awareness

Regular information security awareness must be contacted to make employee security conscious. It is important for every organisation, especially government departments, to ensure that employees who handle classified information receive security awareness.

5.4.16 Lack of training

Government departments should put more emphasis on training to ensure that they train their employees on how to protect sensitive information. If all employees should acquire an appropriate skills and knowledge on how to protect sensitive information, the risks associated with the protection of security information will be mitigated.

5.4.17 Poor management

Top management should support Information Security Managers in complying with security directives such as “MISS”, “MPSS” and security risk control measures for the protection of security information.

5.4.18 Insufficient security budget

Government departments should ensure that they increase their security budget so that Information Security Managers could be able to purchase or install security risk control measures such as electronic devices that will assist security officials to control access to registries where classified information is stored.

5.5. RECOMMENDATIONS FOR FURTHER RESEARCH

It is recommended that further studies be conducted on the relevancy of the “MISS” document and its implementation. This study only focused on the security aspects of the “MISS” document and not the relevance of it. Since the “MISS” document was approved by the government of the Republic of South Africa, its relevance was not researched, hence, the recommendations for further research. This kind of study could establish more security standards relevant to the “MISS”, which could be used to better the protection of security information in government departments.

5.6. CONCLUSION

Government departments have valuable information that needs to be protected. Thus, it is the responsibility of every government employee including top management to ensure that Security Risk Control Measures are applied in full for the protection of security information. The study revealed that the protection of security information in government departments is not being implemented in full to reduce loss, destruction, alteration and leakage of information. Specific reference was made to the "MISS" document that was approved on December 4, 1998 by the South African Government as a national information security policy to be adhered to. These standards must be considered by government departments to ensure proper handling of sensitive or classified information to protect it against loss or destruction. The recommendations discussed in this chapter will assist government departments for the protection of security information.

LIST OF REFERENCES

Axelrod, C. W. 2004. *Outsourcing Information Security.* Norwood: British Library Cataloguing Publisher.

Barker, R.L. 2003. *The social work dictionary,* 5th ed. Washington, DC: NASW Press.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* USA: Cornell University Press.

Buchalter, A.R. 2004. *Law and regulations governing the protection of sensitive but unclassified information.* Washington: Library of Congress.

Bragg, S. 2014. *Accounting practice definition and usage.* Available at: http://www.accountingtools.com/questions-and-answers/accounting-practice-definition-and-usage.html (accessed on 09/08/2015).

Brotby, W. K. 2008. *Information Security Governance: Guidance for Information Security Managers.* Rolling Meadows: T Governance Institute.

Carroll, J. M. 1977. *Computer Security*. 3rd ed. Butterworth: Heinemann.

Chikane, R. 2013. *The things that could not be said*. Johannesburg: Picador Africa Publishers.

Delport, C.S.L. & Roestenburg, W.J.H. 2011. Quantitative data-collection methods: questionnaires, checklist, structured observation and structured interview schedules, pp. 171-205. In De Vos, A.S., Strydom, H., Fouchė, C.B. & Delport, C.S.L. 2011. *Research at grass roots.* Pretoria: Van Schaik Publishers.

Dhillon, G. 2011. *Information Security Management: Global Challenges in the New Millennium.* Pennsylvania: Idea Group Publisher.

Edwards, L. & Brown, I. 2009. Information Security, Law, and Data-Intensive Business Models: Data Control and Social Networking: Irreconcilable Ideas, pp. 202-227. In Matwyshn, A. M. 2009.*Harboring Data: Information Security, Law, and the Corporation.* California: Stanford University Press.

Foster, M. 2012. *Providence Health & Security.* Available at: http://www.sans.org/reading_room/whitepapers/assurance/ (accessed on 03/10/2012).

Fouchė, C.B. & Delport, C.S.L. 2011. In-depth review of literature, pp. 133-140. In De Vos, A.S., Strydom, H., Fouchė, C.B. & Delport, C.S.L. 2011. *Research at grass roots.* Pretoria: Van Schaik Publishers.

Frerk, G., Ypeij, A. & König, R. S. 2014. *Gender and Conflict: Embodiments, Discourses and Symbolic Practices.* England:Ashgate Publishing Limited.

Goodbody, L. 2003. *A Practical guide to Data Protection Law in Ireland.* Dublin: Round Hall Ltd Publishers.

Gutwirth, S., Leene, R., De Hert, P. & Poulett, Y. 2012. *European Data Protection: In Good Health.* London New York: Springer Verlang Publishers.

Greef, M. 2011. Information collection: interviewing, pp. 341-375. In De Vos, A.S., Strydom, H., Fouchė, C.B. & Delport, C.S.L. 2011. *Research at grass roots.* Pretoria: Van Schaik Publishers.

Jay, R. & Hamilton, A. 2003.*Data Protection: Law and Practice.* 2nd edition. London. Australia: Sweet & Maxwell Publisher.

Knight, J., Chilcott, S. & McNaught, M. 2012.*Canada Personal Information Protection and Electronic Documents Act: Quick Reference.* Canada: Thomson Reuters Printers.

Landoll, D. J. 2011. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Assessment.* New York: CRC Press

Layton, T, P., 2007. *Information Security: Design, implementation, measurement, and compliance.* New York: Auerbach Publishers.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: planning and design.* 8th edition. Ohio: Merrill Prentice Hall.

Le Veque, V. 2006.*Information Security: A strategic Approach.* Wiley-Interscience
Carey, P. 2000. *Data Protection in the UK.* United Kingdom: Blackstone Press Limited Publishers.

Lombard, A. 2002. *The professional status of social work.* Social work / Maatskaplike Werk. Stellenbosch: University of Stellenbosch.

Mackenzie, M, H. 2012. *Female Soldiers in Sierra Leone: Sex, Security, and Post, Conflict Development.* New York and London: New York University Press.

Mason, J. 1996. *Qualitative Researching*. London: SAGE Publications.

Mistry, D., Minnaar, A., Patel, C. & Rustin, C. 2003. *Criminal Justice Research Methodology.* Pretoria: Technikon SA.

Morgan, R. & Boardman, R. 2003. *Data Protection Strategy: Implementing Data Protection Compliance.* London: Sweet & Maxwell Publishers.

Mulder, G. 2006. Guide to security threat and risk assessment. *Paper presented at the National Intelligence Agency security management course, Roodeplaat,* June.

Northrup, C. L. 2006. *Information security: A corporate governance.* Fort Lauderdale: J. Ross Publishers.

Olsen, W, P. 2010. *The Anti-Corruption Handbook: How to protect Your Business in the Global Marketplace.* Canada: John Wiley & Sons Inc. Publishers.

Oosthuizen, G. C., Shapiro, H. A. & Strauss, S, A. 1983. *Professional Secret in South Africa.* Cape Town: Oxford University Press.

Peltier, R. T., Peltier, J. & Blackley, J. 2005.*Information Security Fundamentals.* New York: Auerbach Publishers.

Prunckun, H. W. 1989. *Information security: A practical Handbook on Business Counterintelligence.* Springfield: Charles C Thomas Publishers.

Quigley, M. 2005. *Information Security & Ethics: Social & organisational issues.* USA: IRM Press.

Raggad, B. G.2010. *Information Security Management.* New York: Auerbach Publisher.

Reddick, C. G. 2012. *Public Administration and Information Technology.* Canada: Jones & Bartlett Learning.

Rogers, C. 2008. A security risk management approach to the measurement of crime in a private security context: Acta Criminological. *Southern African Journal of Criminology. Crimsa 2008 Conference Special Edition (3) 2008*. Pretoria: University of South Africa.

Rogers, F.C. 2005. *Security Practice III/Security Risk Management IV: SEP361S/SRM401S.*2nd ed. Florida: Technikon SA.

Rosenberg, J., & Mateos, A. 2011. *The cloud at your service.* Washington: Minning Publishers.

Ross, J. I. 2000. *Controlling State Crime.* 2nd edition. New Brunswick: Transaction Publishers.

Rowe, E. A. 2009. Information Security and Trade Secrets: Dangers from the Inside: Employees as Threats to Trade Secrets, pp. 92-99.In Matwyshn, A. M. 2009.

Harboring Data: Information security, Law, and the Corporation. California: Stanford University Press.

Silverstone, H. & Sheetz, M. 2007. *Forensic Accounting and Fraud Investigation for Non-expert.* 2nd edition. New Jersey: John Wiley & Sons, Inc.

Solove, D. J. & Schwartz, P, M. 2011. *Privacy Law Fundamentals.* USA: IAPP Publishers.

South Africa. 1982. *Protection of Information Act 82 of 1982.* Government Gazette 32999. Pretoria: Government printer. 5 March.

South Africa. 1998. *Minimum Information Security Standards.* 2nd edition., March 1998. Available at: http://www.right2info.org/resources/publications /laws-1/SA_Minimum%20Information%20Security%20Standards.pdf (accessed on 16/11/2012).

Schurink, W., Fouché, C.B. & De Vos, A.S. 2011. Qualitative data analysis and interpretation, pp. 397-423. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grass roots.* Pretoria: Van Schaik Publishers.

Schweitzer, J. A. 1996. *Protecting Business Information: A manager's Guide.* West Yorkshire: British Library Cataloguing Publishers.

Strydom, H. & Delport, C.S.L. 2011. Information collection: document study and secondary analysis, pp. 376-389. In De Vos, A.S., Strydom, H., Fouchė, C.B. & Delport, C.S.L. 2011. *Research at grass roots.* Pretoria: Van Schaik Publishers.

Tesch, R. 1992. *Qualitative Research. Analysis Types & Software Tools.* London: The Falmer Press.

Tipton. H.T. and Krause. M. *Information Security Management Handbook*. 3rd edition. USA: Auerbach Publishers.

Tucker, G. 1992. *Information Privacy Law in Australia.* USA: Longman Professional Publisher Publishers.

Van der Westhuizen, A., Schellnack-kelly, I & Geyer, R. 2010. *Basic Archives and Records Management course.* South Africa: UNISA Centre for Applied Communication.

UNISA Policy on research ethics, 2007. Available at:

https://my.unisa.ac.za/tool/a87dd927-a9e0-4b59-0012-5ab7d72ca660/contents/colleges/col_grad_studies/docs/Policy_research_ethics_21September2007.pdf (Accessed on 13/12/2012).

Urdang, L. 1995. *The Oxford Desk Dictionary.* New York: Oxford University Press.

Walsh, A. & Hemmens, C. 2011. *Introduction to Criminology*: A Tex / Reader. 2nd edition. USA: SAGE Publication Ltd.

Whitman, M. E. & Mattord H, J.2008. *Management of Information Security.* 2nd edition. Canada: GEX Publishing Services.

ANNEXURES

Annexure A: Interview schedule

INTERVIEW SCHEDULE

PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA

Please answer all of the following questions as honestly as possible. The information collected during this study will be used to help the researcher to come up with constructive solutions for the lack of security measures with regard to protection of security information by government departments. You do not need to identify yourself and the researcher undertakes to maintain anonymity in that there is no possibility of being identified or linked in any way with the research findings in the final research report. Where required please indicate your answer with a cross (X) in the appropriate box.

SECTION A: DEMOGRAPHIC DATA

The following questions are for statistical purposes only:

1. Gender

Male	
Female	

2. Age range

15-25	
26-35	
36-45	
46- and above	

3. The highest educational level attained:

None	
Grade 1 up to grade 7	
High School	
Undergraduate	
Postgraduate	

4. Employment category:

Clerical	

Administration	
Junior Management	
Middle Management	
Top Management	

5. Name of your institution or / department:

State security	
Correctional services	
Home Affairs	
Police	
Defence and military veterans	
Justice and Constitutional Development	
Other (please specify):	

SECTION B: SECURITY RISK CONTROL MEASURES

6. What type of security risk control measures are in existence for the protection of security information in Government Departments?

....
....

7. Do you find the security risk control measures at your department to be effective?

Yes		No	

8. If no, please say why you find these measures to be not effective.

....
....

Indicate to what extent you agree or disagree with the following statements:

9. Leakage of information at Government department can be reduced if proper security risk control measures can be implemented effectively by Security Managers (SM)

Strongly agree		Agree		Neutral		Disagree		Strongly disagree	

10. Do you have security policies and procedures in place at your department pertaining to protection of security information?

Yes		No	

11. If ‘yes’ how familiar are you with these security policies and procedures that are in place?

....
....

12. How access to the registry is controlled in your department?

....
....

13. How do you exercise control over outgoing and incoming classified documents?

Outgoing registers	Yes	No
Incoming registers	Yes	No
Outgoing classified registers	Yes	No
Incoming classified registers	Yes	No
None of the above	Yes	No

Any other/specify..
....

14. How are classified documents removed or dispatched from the premises? (E.g. securing transportation methods, records keeping and authorization).

....
....

15. What security programmes are in place to make the staff security conscious with regard to protection of security information?

....
....

SECTION C: SECURITY RISKS IN GOVERNMENT DEPARTMENTS

16. What security risks are associated with the protection of security information in Government Departments?

....
....

17. Did you ever experience theft of information in your department?

Yes		No	

18. If ‘yes’ please indicate below how this information was stolen in your department.

1		2	3	4	5
Theft of computers and laptops from offices					
Theft of laptops from official’s own vehicles					
Missing files from registry					
Burglary in offices					
Corruption by internal employees					
Interception from computers/ computer hacking					

19. Did you report any of these experienced crime/ theft of information?

Yes		No	

20. If ‘yes’, to whom did you report these crime/theft of information?

Police		State Security Agency		Head of Department		Manager/supervisor	

21. Was any action taken after this incident or theft of information was reported?

Yes		No	

22. If ‘yes’, please specify what was done:

....
....

23. Do all personnel handling sensitive information in your department have a valid security clearance certificates?

Yes		No	

24. If ‘yes’ please indicate the level of the security clearance they have.

Top secret		Secret		Confidential	

25. How all employees or sections within the department are receiving their mail and official files? (Do they sign for it, is there a checklist for the mail and etc).

Signing mail register		Security envelopes		Hand delivered		Non- security envelopes/ files	

26. Are there security risk control measures in place when photocopying classified documents?

Yes		No	

27. If 'yes' please specify:

....
....

28. Are there security risk control measures when the destruction of redundant documents containing sensitive information is done?

Yes		No	

29. If 'yes" please specify the type of security risk control measures:

....
....

30. Are communication equipment protected for interception in your department?

Yes		No	

31. If 'yes' please explain how is it protected:

....
....

32. Are there safes, strong rooms or re-enforced steel cabinets for the storage of classified documents in your department?

Yes		No	

33. If 'no' please indicate how are classified documents stored in your department:

....
....
....
....

34. Is access to computer/saver/network room controlled?

Yes		No	

35. If ‘yes” please specify how it is controlled:

....
....

36. Do computer users protect information stored in their computers?

Yes		No	

37. If ‘yes’ please specify how computer users protect information stored in their computers:

....
....

38. Have you ever been approached by outside people requesting you to provide government information in exchange of money or anything?

Yes		No	

39. If ‘yes’ please explain:

....
....

SECTION D: SOLUTIONS ON THE PROTECTION OF SECURITY INFORMATION IN GOVERNMENT DEPARTMENTS

40. Which type of security risk control measures may be put in place for the protection of security information in Government Departments?

....

....

....

41. In your opinion, what should be done to improve the protection of security information in general in your department?

....
....

………………………………………………………………………………………………………
………………………………………………………………………………………………………

42. What security risk control measures do you think need to be changed in YOUR department to make them more effective for the protection of security information?………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………
………………………………………………………………………………………………………

For office use:

Questionnaire number:……………………………………

Researcher’s Signature:……………………………………

Date of interview:…………………………………………

ANNEXURE B: OBSERVATION CHECKLIST

OBSERVATION CHECKLIST

Security measures surveyed: Government departments			
Survey date			
	Yes	**No**	**Comments**
1. Are there approved security policy document for the protection of security information?			
2. Are doors at registry office in which classified documents are kept fitted with security locks?			
3. Are there course materials, security manuals and posters in place?			
4. Are there registers for incoming and outgoing classified documents?			
5. Are there security legislations applicable for the protection of security information?			
6. Are classified documents that are not in use stored in the appropriate safe storage facilities such as normal filing cabinet, reinforced filing cabinet, safes or walk in safes and strong room?			
7. Are there physical protection systems such as access control to registries, safes, strong rooms, reinforced filing cabinets and visitor’s cards in place?			
8. Are there effective access control to restricted areas such as cryptographic, server room and computer centres?			
9. Are there proper control over movement of classified information in the registry office?			
10. Are documents containing sensitive information classified according to their level of classification?			
11. Does the department uses secure transportation when transporting classified documents?			
12. Are receipts signed by the addressee and returned to			

sender when classified documents were delivered?			
13. Are there registers for photocopying of classified documents?			
14. Are there registers for the destruction of classified documents?			
15. Do employees sign for their office keys?			
16. Are there security alarm s implemented at Registry Office?			
17. Are there records kept for security meetings?			
18. Are personal files of every employee classified?			
19. Are records kept for all departmental files that contain sensitive information?			
20. Are there records kept for confidentiality agreements or oath of secrecy?			
Subtotal			
A: Total “yes” answers:			
B: Total “no” answers:			
Security backlog (weakness)			

ANNEXURE C: DOCUMENTARY CHECKLIST

DOCUMENTARY CHECKLIST

Security measures surveyed: Government departments			
Survey date			
	Yes	**No**	**Comments**
Do you have security policy?			
Is this security policy implemented effectively?			
Is the security policy renewed annually?			
Does your security policy cover the protection of security information?			
Do you have security manuals or posters?			
Are there security procedures in place?			
Do you have security plan?			
Is the security plan implemented effectively?			
Do you have access to internet?			
Do you have course materials for the courses that you attended?			
Are there applicable security legislations?			
Do you keep records or minutes of security meetings?			
Does every employee have personal file?			
Do you keep records of all departmental files that contain sensitive information?			
Do you keep records of government publications?			
Do you keep records of conference papers?			
Do you keep records of security reports?			
Subtotal			
A: Total “yes” answers:			
B: Total “no” answers:			
Security backlog (weakness)			

Annexure D1 to D14: Permission letters to conduct interviews in government departments.

DEPARTMENT OF CRIMINOLOGY AND SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Director: Domestic Branch SSA
Mr S J Ntombela
State Security Agency
Musanda
Private bag x 87
Protoria
0001

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master’s degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

UNISA college of law

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of department
MS D Seketane
Department of Health
11Masanatrust
BUSHBACHRIDGE
1285

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master’s degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of department
Mr Abe Abraham
Department of Water Affairs
28 Central road
Northen Cape
Kimberley
8300

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Captain Masebe
South African Police Service
GERMISTON
69 Railway Road
GERMISTON
1400

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with

the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of Department
Mr Victor Constable
Department of Rural Development
4 Henshel Street
Medicine building
NELSPRUIT
1300

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of Department
Mr Bongani Gxilishe
Department of Economic Development,
Environmental Affairs and Tourism
Cnr Beacon Hill and Hargreaves Road
Hockley close
KING WILLIAMS TOWN
5600

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of Department
Mr Ceba Mthoba
Department of Agriculture, Forestry and Fisheries
Fortrust Building
Martin Hammerschlag Way
Roggebay
CAPE TOWN

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with

the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Brigadier N. Ramaila
South African Police Service
POTCHEFSTROOM
7&8 Du Bros Building
Crn Sol Plaatjie and James Moroka
POTCHEFSTROOM
3521

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with

the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND	Preller Street, Muckleneuk Ridge
SECURITY SCIENCE	City of Tshwane
SCHOOL OF CRIMINAL JUSTICE	PO Box 392
COLLEGE OF LAW	UNISA
UNISA	0003
Tel: (+27) (0)12-433 2164	South Africa
Fax: (+27) (0)12- 4296609 6641	
e-mail: govend1@unisa.ac.za	

10 May 2014

The manager
Mr Z Lekola
Frestate Department of Health
P.O.Box 227
Bloemfontein
9300

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Cluster Commander
Major General: MCcRacken
South African Police Service
PORT NOLOTH
Northern Cape
8300

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with

the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Station commander
South African Police Service
CYFERSKUIL
RADIUM
0783

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Advocate Winnie Sonti
Department of Justice and Constitutional Development
72 Bok Street
POLOKWANE
0700

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

Commissioner T B Seruwe
Department of Labour
94 W F Nkomo Street
PRETORIA
0001

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master’s degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Tel: (+27) (0)12-433 2164
Fax: (+27) (0)12- 4296609 6641
e-mail: govend1@unisa.ac.za

Preller Street, Muckleneuk Ridge
City of Tshwane
PO Box 392
UNISA
0003
South Africa

10 May 2014

The Head of department
Mr S Mokoko
Northern Cape Provincial Treasury
Cnr Stead & Knight Street
Private bag x 5054
KIMBERLY
8300

Dear Sir/Madam

PERMISSION TO CONDUCT EMPIRICAL RESEARCH: STUDENT: MJ NKWANA: TITLE OF DISSERTATION: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master's degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the risks.

An empirical study will be conducted by the researcher to collect information with regards to the above mentioned study. Permission is requested for Mr Nkwana to conduct one – one interviews, observation and documentary study at your premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana's supervisor, Prof D Govender: 012 4339482: e-mail: govend1@unisa.ac.za , at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Herewith, please find ethical clearance certificate issued by UNISA to conduct this research.

Mr Nkwana's contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

Regards

Govender

____

Doraval Govender (Dr)

Associate Professor: Programme Security Management

Annexure E: Informed consent letter to conduct interviews.

CONSENT FORM

AGREEMENT:

I hereby consent to:

	Yes	No
43. Being interviewed on the following topic: **Protection of security information within Government Departments in South Africa**		
44. To give honest answers to reasonable questions and not to mislead the interviewer/ researcher;		
45. The interview being tape recorded to ensure that valuable information elicited during the interview is adequately captured and the context of information can be reviewed in details.		

I also understand that:

46. This is a voluntary participation;

47. I may withdraw from participation at any time should I want to do so;

48. My opinion will be viewed as strictly confidential. Anonymity is guaranteed and no data published in dissertations and journals will contain any information through which my name as an interviewee may be identified;

49. No reimbursement or gift will be received from the researcher in respect of information rendered;

50. I indemnify the researcher /interviewer against any liability that I may incur during the course of the research project;

51. I have received a signed copy of this consent form;

I hereby acknowledge that the researcher:

52. Explained and discussed in details the main aims and objectives of the research project with me;

I am fully aware of:

53. the serious consequences that may follow any breach or contravention of this consent;

In co-signing this agreement the researcher undertakes to:

54. maintain confidentiality, anonymity, and privacy regarding the identity of the interviewee and information rendered by him/her.

Signature of participant (interviewee): ………………………….

Signed at …………………on……………………...

Signature of researcher (interviewer): ………………………….

Signed at …………………on……………………...

I certify that the interviewee has acknowledged that he/she understands the contents of this consent which was signed before me and that content of this document was explained and discussed with the interviewee:(interviewer signature):…………………….

Annexure F: Permission letter to conduct the study

UNISA college of law

COVER LETTER

DEPARTMENT OF CRIMINOLOGY AND
SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE
COLLEGE OF LAW
UNISA
Te: +27 12 429 2164
Fax: +27 12 429 6609
E-mail: govend1@unisa.ac.za

Preller Street
Muckleneuk Ridge
PRETORIA
P.O. Box 392
UNISA
0003
South Africa

08/05/2014

TO WHOM IT MAY CONCERN

Dear Sir/Madam

TITLE OF THE RESEARCH PROJECT: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA.

Mr Mokata Johannes Nkwana is currently a registered student busy with his research studies for master’s degree (M Tech) at the University of South Africa (UNISA) in the Department of Security Risk Management, School of Criminal Justice, College of Law.

The purpose of this research is to evaluate the existing security measures at government departments in South Africa, to identify the risks associated with the protection of information, so that appropriate security risk control measures may be recommended to mitigate the threats.

An interview schedule will be used by the researcher to collect information on the above objectives with regard to the above mentioned research topic. Your department’s participation in this study will help the researcher with his study. We therefore request permission for Mr Nkwana to conduct semi-structured interviews, observation and documentary study at you premises together with your employees.

Kindly be informed that responses from participants will be treated as confidential. Respondents/ participants are not required to identify themselves in the questionnaire.

Should there be any enquiries about this research project, please do not hesitate to contact Mr Nkwana’s research supervisor, **Prof D Govender** (012 4339482), or Prof A dev Minnaar (012 4339530) at the Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA, South Africa.

Mr Nkwana’s contact details are as follows: Tel: 012 337 1141; Cell: 071 380 8563

Thanking you for your cooperation.

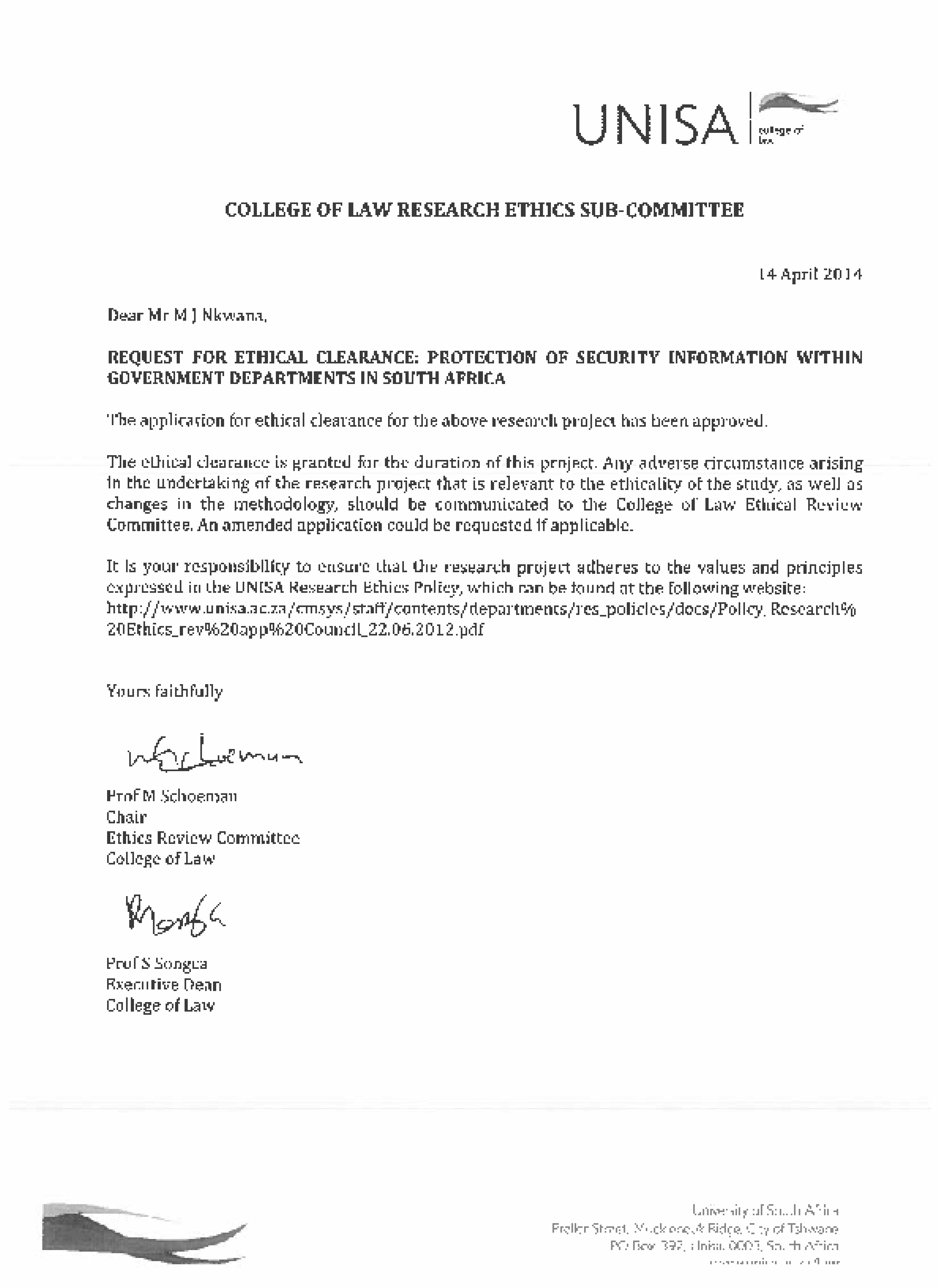
Regards

Govender

(Prof) **Doraval Govender**

Associate Professor: Programme Security Management

Annexure G: Ethical Clearance Certificate



UNISA college of law

COLLEGE OF LAW RESEARCH ETHICS SUB-COMMITTEE

14 April 2014

Dear Mr M J Nkwana,

REQUEST FOR ETHICAL CLEARANCE: PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA

The application for ethical clearance for the above research project has been approved.

The ethical clearance is granted for the duration of this project. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated to the College of Law Ethical Review Committee. An amended application could be requested if applicable.

It is your responsibility to ensure that the research project adheres to the values and principles expressed in the UNISA Research Ethics Policy, which can be found at the following website: http://www.unisa.ac.za/cmsys/staff/contents/departments/res_policies/docs/Policy_Research%20Ethics_rev%20app%20Council_22.06.2012.pdf

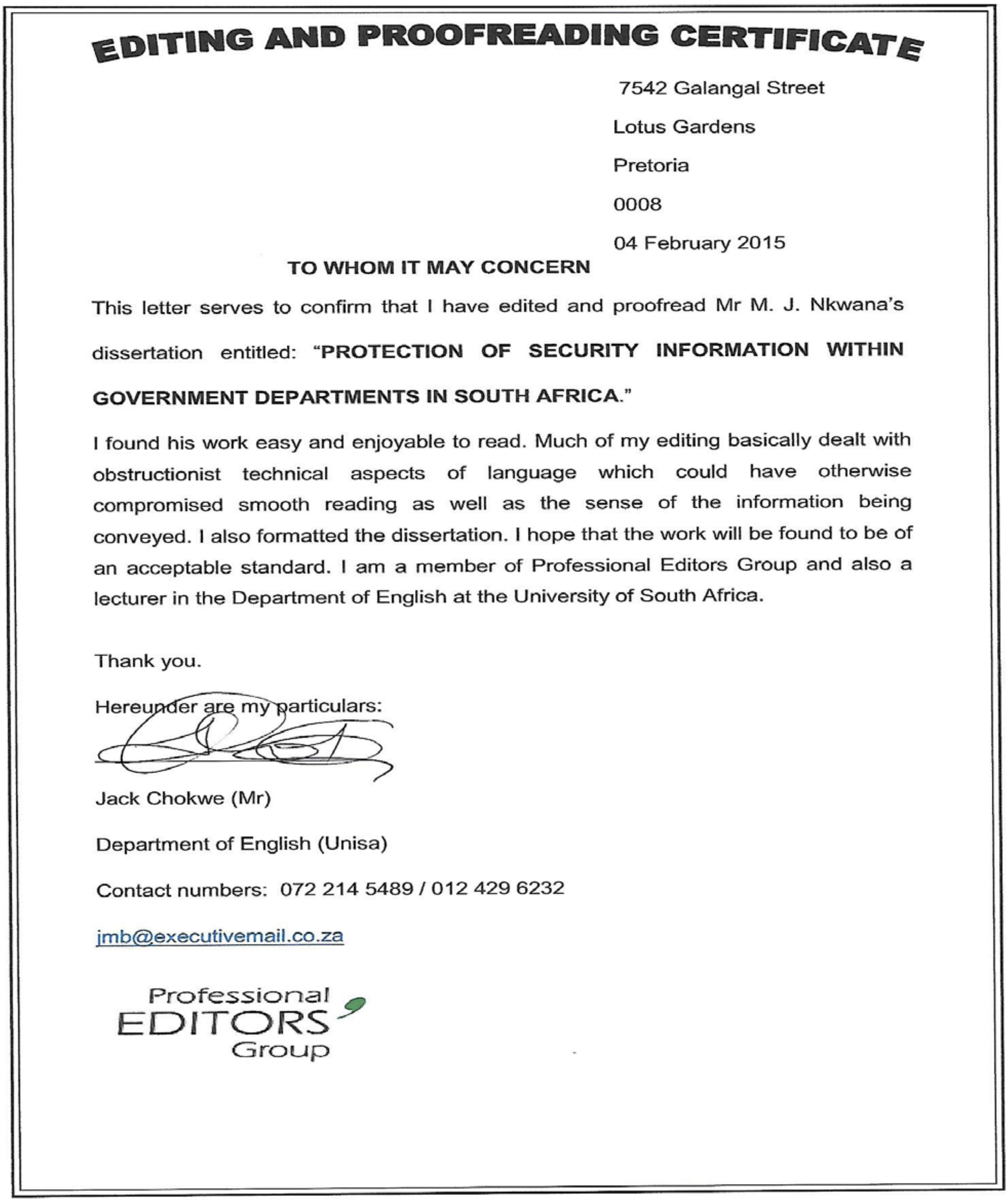
Yours faithfully

Prof M Schoeman
Chair
Ethics Review Committee
College of Law

Prof S Songca
Executive Dean
College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, Unisa, 0003, South Africa
www.unisa.ac.za

Annexure H: Editing Certificate



EDITING AND PROOFREADING CERTIFICATE

7542 Galangal Street
Lotus Gardens
Pretoria
0008
04 February 2015

TO WHOM IT MAY CONCERN

This letter serves to confirm that I have edited and proofread Mr M. J. Nkwana's dissertation entitled: "**PROTECTION OF SECURITY INFORMATION WITHIN GOVERNMENT DEPARTMENTS IN SOUTH AFRICA**."

I found his work easy and enjoyable to read. Much of my editing basically dealt with obstructionist technical aspects of language which could have otherwise compromised smooth reading as well as the sense of the information being conveyed. I also formatted the dissertation. I hope that the work will be found to be of an acceptable standard. I am a member of Professional Editors Group and also a lecturer in the Department of English at the University of South Africa.

Thank you.

Hereunder are my particulars:

Jack Chokwe (Mr)

Department of English (Unisa)

Contact numbers: 072 214 5489 / 012 429 6232

jmb@executivemail.co.za

Professional
EDITORS
Group