Investigating Factors of Non-compliance of information security management in Public Sector, South Africa

Tania Abrahams

A research report submitted to the Faculty of Commerce, Law and Management, University of Witwatersrand, in partial fulfilment of the requirements for the degree of Masters of Management in Public Development Management

Johannesburg, 2012

(April 2012)

ABSTRACT

Cybercrime is on the increase and rampant globally. Although we have implemented various mechanisms, international agreements, legislation and policy documents, we are unable to combat this phenomenon. Public Service is inherently dependant on the availability, integrity and confidentiality of its mission critical information to deliver an effective and efficient service to the citizens of the SOUTH AFRICA. This is informed by key legislative requirements and policy documents to ensure information is protected and secured, to avoid and minimise risks. SOUTH AFRICA has legislation that compels compliance and it is a matter of state security that information is protected and preserved.

The increased usage of information and communication technologies in the public service have exposed and made the institution vulnerable to potential intrusions. Global trends indicate that Senior Managers are not implementing information security policies and procedures. Although policies and procedures exist for the secure control of information it is not known how high their awareness levels are to ensure the procedures are operationalised.

The purpose of this research is to investigate factors of non-compliance of information security management in the Public Service of South Africa.

The researcher followed a scientific research methodology process by developing a problem and purpose statement. With the aid of the literature review the researcher was able to formulate Hypothesis, with the key themes focussing on adherence of governance and international standards, employee information security awareness and roles and responsibilities of employees when handling government information, based on Minimum Information Security Standards that provide procedures and standards to protect information.

It is crucial to achieve the highest level of compliance, as this will entrench a culture of security conscience public service managers. With the advent of government developing a security framework, this research could make a meaningful contribution to that framework, as it would highlight areas that require immediate intervention with limited resources.

Key Words:

Information Security Management, Compliance, Public Sector, Information and Communication Technologies, Corporate Governance, IT Governance, Information Security Governance, International Information Security standards.

DECLARATION

I, Tania Abrahams, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Masters of Management for Public Development Management in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Tania Abrahams

Signed at _____

On the _____ day of _____2012.

DEDICATION

This research report is dedicated to my children, my son Jody and daughter Alex. Thank you for your patience, understanding and making me the person that I am today. Your love and support has made me to persevere.

ACKNOWLEDGEMENTS

I wish to thank and express my sincere gratitude and appreciation to the following people:

- My supervisors, Dr Johnny Matshabalapala and Mr Rabelani Dagada, for the patience, support, guidance, assistance and motivation provided to me throughout my research process,
- My friend Regi, who has been a source of inspiration,
- To my children, for the all sacrifices, without your support, I would not have made it thus far. May this inspire you to reach for the stars
- Finally, the participants in my questionnaire, without them this research would not have been possible.

TABLE OF CONTENTS

LIST OF FIGURES

List of Abbreviations and Acronyms

B2B	Business to Business relationships
CIO	Chief Information Officer
ECT	Electronic Communications and Transaction
ERP	Enterprise Resource Planning
HOD	Heads of Department
ICT	Information Communication Technology
IS	Information Security
ISG	Information Security Governance
ISM	Information Security Management Systems
IT	Information Technology
ITG	Information Technology Governance
MISS	Minimum Information Security Standards
PWC	Price WaterHouse Coopers
USA	United States of America
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DOD	Department of Defence
ISP	Internet Service Provider
NASA	National Aeronautics Space Administration
CIA	Central Intelligence Agency
BSI	British Standards Institute
ISG	Information Security Governance

List of Definitions

Accreditation - is the procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.

Certification- is written assurance by a third party that a product, process or service conforms to specified requirements.

Cyber crime – the threats in the digital world mirror the threats in the physical world such as theft, racketeering, vandalism, voyeurism, exploitation, extortion, con games and fraud. There's even the threat of physical harm.

DDos (Distributed denial-of-service) – are just a virulent strain of DoS attacks, meaning there is no single source of the attack. Denial-of-service does harm just by the attempt to deliver packets; whether or not the packets would authenticate properly is completely irrelevant. They stop something from working, such as attacks and session hijacking. Denial-of service attacks work because computer networks are there to communicate.

Espionage – the act of spying to obtain information unlawfully.

Globalisation - the growing economic interdependence of countries worldwide through increasing volume and variety of cross-border transactions in goods and services, free international capital flows, and more rapid and widespread diffusion of technology.

ICT- technology that deals with the storage, processing and dissemination of information especially using computers.

Information – is an asset, like other important business assets, has value to an organization and consequently need to be suitably protected.

IS – the protection of information and the systems and hardware that use, store and transmit that information to ensure business continuity, minimize

business damage and maximize return on investments and business opportunities.

Fraud – deliberate deception or cheating intended to gain an advantage. Fraud has been attempted against every commerce system ever invented; neither will the criminals' techniques.

Phishing scams - the act of sending an e-mail falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft

Regulatory - restricting according to rules and principals

Research – involves the application of various methods and techniques in order to create scientifically obtained knowledge by using objective methods and procedures.

Spam - the sending of unsolicited bulk e-mail- that is, email that was not asked for (unsolicited) and received by multiple recipients (bulk).

Standard – is a technical or procedural specification, or both, that is significant and should be followed.

Chapter 1 - Introduction

1.1 Introduction

Cybercrime is on the increase and rampant globally. Although we have implemented various mechanisms, international agreements, legislation and policy documents, we are unable to combat this phenomenon. However the international standards have identified compliance with own defined policies and information security awareness as one method of increasing vigilance amongst employees who handle confidential information on a daily basis.

The researcher followed a scientific research methodology process by developing a problem and purpose statement. With the aid of the literature review the researcher was able to formulate hypothesis, with the key themes focussing on adherence of governance and international standards, employee information security awareness and roles and responsibilities of employees when handling government information, based on Minimum Information Security Standards that provide procedures and standards to protect information.

The researcher identified quantitative research through stratified sampling as the most appropriate method. The researcher targeted senior managers who have a direct responsibility and involvement in ensuring compliance with information security policies. The researcher sampled 100 (n) respondents of the entire population that is constituted by HOD's, CIO's, IT Managers, IT Security Managers, IT Security Consultants, IT Specialist and Lines of Business Managers. The researcher collected primary data with use of the survey questionnaire as an instrument and secondary data by reviewing appropriate literature in books, journals, case studies and articles. Data analysis through manipulation and organising of data will reveal the truth about the research conducted. The research would be deemed reliable if you are able to conduct the same research over and over again attaining the same results.

Discovery and Implementation as conceptualised by Leedy (1993), will be the primary focus to investigate factors of non-compliance of information security management in the public sector of South Africa and subsequently interpret

the results obtained from an in-depth analysis of the data. The research report will consist of 6 chapters.

Chapter 1 Introduction

The introduction includes the background of the research, problem statement and purpose statement.

Chapter 2 Literature review

A comprehensive literature review of legislative aspects in South Africa relevant to information security, international norms and standards with respect to security management and best practices has been conducted. The researcher compiled an introduction, incorporated definition of terms and the main content that consists of information security related crime defined, legal aspects of IS and ISM.

Chapter 3 Research methodology

In this chapter the researcher outlined the research approach, research design, data collection, data analysis and validity and reliability followed.

Chapter 4 Data Presentation

The feedback received from the survey questionnaire has been analysed, the researcher is able to present findings in statistical format, with graphs and charts.

Chapter 5 Analysis of Data

The researcher presents an analysis of the data, post the statistical analysis.

Chapter 6 Conclusions and Recommendations

The researcher highlights the research problem to the reader and motivate whether the purpose of the research was achieved. The researcher forwarded recommendations based on findings.

1.2 Background

According the Minister of State Security, Dr Cwele, *"The forging of identity and other official government documents, the penetration of our information and communication technologies systems to perpetrate fraud; the break-ins in a number of strategic state entities; the selected and distorted leakage of state information to destabilise and sow division; all negatively impact on the state's ability to function and to deliver much needed services to our people. We must ensure that all sensitive state information is properly managed, controlled and protected from theft, manipulation, cyber attack and unauthorised disclosure, be it from corrupt officials, criminal syndicates, foreign adversaries or information pedlars." (2009)*. Public Service is inherently dependant on the availability, integrity and confidentiality of its mission critical information to deliver an effective and efficient service to the citizens of the South Africa. This is informed by key legislative requirements and policy documents to ensure information is protected and secured, to avoid and minimise risks. South Africa has legislation that compels compliance and it is a matter of state security that information is protected and preserved. Legislation that speaks to the preservation and protection of information as a key asset to state are the Public Service Act, the Electronic and Communications Act, Copyright Act and governments policy document MISS.

The increased usage of information and communications in the public service have made the institution vulnerable and exposed it to the potential risk of intrusions. These risks include elements of cybercrime such as hacking, viruses and spam. South Africa has not been immune to such phenomenon and fell prey to one such instance during 2004 (Sophos.com, 2004). The Sasser virus crippled the institution which resulted in the shutdown of governments' information and communication networks which had dire effects on service delivery throughout the country. Other instances where the recent spate of hoax e-mails that affected members from the highest office in the country, namely Presidency (Polity.org, 2006). It is for this reason that the preservation and protection of information, as a critical asset should be a priority on the agenda of public service.

One of the worlds' leading independent authorities; (Information Security Forum et. Al ENISA, 2007), says, "*Information security awareness is an*

ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change."

1.3 Problem Statement

The increased usage of information and communication technologies in the public service have exposed and made the institution vulnerable to potential intrusions. Global trends indicate that Senior Managers are not implementing IS policies and procedures, although trends in the governance arena highlights the elevation of ISG to board of director and executive management levels, to ensure compliance with organisational policies. South Africa have implemented the MISS with an objective to provide procedures and measures to protect government information that will impact the vulnerability of state should it be compromised, however a study conducted by Dagada, Eloff and Venter (2009) found that most organisations and government departments do not take IS seriously. Many organisations have IS policies in place; however these were purchased off-the-shelve to ensure compliance with ISO2700 standards, and to gain certification.

1.4 Purpose Statement

The purpose of this research is to investigate factors of non-compliance of information security management in the public sector of South Africa. The researcher would then present the findings, interpret and analyse findings on the management of information security. The following research questions were explored:

- What are the factors leading to non-compliance in the management of IS in the public sector of South Africa?
- What are the trends to ensure compliance of IS?
- What are the strategy configurations in managing IS in the public sector of South Africa?

The contribution of the research report moreover recommends ways to enhance IS capability of public sector. It proposes ways to install a built-in IS mechanism to ensure greater accountability of senior managers to ensure compliance with MISS.

1.5 Significance of the Study

This study will determine how well Senior Managers in the Public Service comply with the MISS to ensure availability, integrity and confidentiality of information. It is critical to ensure a culture of compliance with IS policies and procedures, thus minimising the risk associated with intrusions and the vulnerability of state information. With the advent of government developing a security framework, this research could make a meaningful contribution to that framework, as it would highlight areas that require immediate intervention with limited resources.

Chapter 2 – Literature Review

2.1 Introduction

To be able to properly understand what will be required to comply with ISM in the public sector of South Africa, the researcher deemed it essential to gain a thorough understanding of corporate governance, IT Governance, ISG, international IS standards; South African legislation and definitions applicable to ISM were reviewed. In the past IS was assigned to the IT Manager, however there has been paradox and it now widely acceptable that all in the employ of the public service, management and staff should contribute to compliance with IS policy. With the acceptance of the Codes of Good Practice, King III Report, Members of the Board of Directors, CEOs and Managers at a strategic level are held accountable for the implementation of IS and executing of oversight responsibility in respect of governance to ensure compliance. These shifts are attributed to global developments in corporate governance and organisational acceptance of IS accountability.

2.2 Understanding the process of Literature Review

The literature review sets the scene for research process, affording the researcher the opportunity to gain insight and an understanding of literature in the field of study (Boote & Beile, 2005). LeCompte, Klinger, Campbell & Menke (2003) states the researcher is able to demonstrate knowledge of the field of study, by reviewing of history, theories, trends and allows the research insight to positions on the subject matter of influential researchers and groups, which would to lead to accepted academic report.

By following prescribed scientific approach, the literature review yields benefits for the research process as it delimits the research problem, eliminates futile approaches, identify recommendations, support grounded theory and the researcher is able to gain insights to methodologies (Gall, Borg & Gall, 1996). Hart (1998) further outlines that the literature review identifies variables relevant to the research problem, synthesizes perspectives and contextualises the research problem.

The literature review is an analysis of information that focuses on findings, whereby the researcherer is able to draw conclusions (Educational Resources Information Centre, 1982).

The research has reviewed literature relevant to ISM and explored literature on corporate governance, IT Governance, ISG, international information security standards; South African legislation and definitions applicable to ISM to determine the impact on factors of non-compliance with IS.

2.3 Role of Governance in Information Security Management

ISM has radically evolved over the last couple of decades, as initially it was characterised by technical aspects, management dimension, become institutional as there was a greater need for standardisation and the fourth wave clarified the role of ISG (von Solms, 2000). Prior to unpacking ISG it is critical to gain insights and an understanding of corporate governance and ITG as through its evolution IS has a significant impact.

2.3.1 Corporate Governance

Globally corporate governance had a significant impact on businesses worldwide, which affects its structures, processes and mechanisms (Wixley & Everingham, 2005). Corporate Governance related to the manner in which an organisation is governed and the technique used to direct and manage the organisational performance, ensuring stakeholder expectations are met (Management Study Guide, 2011). Various stakeholders are critical in achieving the organisations predetermined objectives and these relations between shareholders, members of the board of directors, management, trade unions and employees are necessary to attain the organisations objectives through monitoring of performance (OECD, 2005). Adherence to good principles of corporate governance yields substantial benefits for organisations is it would be able to attract investors, therefore to ensure economic prosperity (Weill, 2004). It is therefore incumbent upon the board of directors to ensure organisations are directed and controlled appropriately to ensure objectives and goals are met to attract and retain future business.

Three key stakeholders, namely the board of directors, executive management and managers; have a direct bearing on the successful implementation of the two core principles of corporate governance (Von

Solms and Von Solms, 2006). It is incumbent upon the board of directors and executive management to determine the vision and mission of the organisation, tactically managers will drive the implementation of such directives and operationally the directives, such as standards, policy and procedures will be implemented.

As organisations are utilising IT tools more widely (Von Solms, 2006) it would be prudent to review literature on ITG. The literature reviewed above has highlighted corporate governance relates to meeting the organisations strategic objectives and this could be achieved if information as an asset is protected.

2.3.2 IT Governance

Petersen (2004) defines ITG as the distribution of IT decision making rights and responsibilities amongst organisational stakeholders and the procedure and mechanism for making monitoring strategic decisions regarding IT. The responsibility of IT governance rests with the board of directors and executive management, as it is integrated with corporate governance (ITGI, 2000; Brown, 2006; Petersen, 2004).

According Van Grembergen, De Haes, & Guldentops (2004) IT governance aligns IT with an organisations strategy to ensure maximum value is derived.

ISACA (2009) further says that IT governance is a component of corporate governance that outlines the responsibilities of the board of directors and executive management to ensure the objectives of the organisation is achieved, through effective and efficient utilisation of organisation resources, taking all possible risks into account. According to ITGI, CobiT best practise frameworks, "*IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT [the infrastructure as well as the capabilities and organisation that establish and support it] sustains and extends the organisation's strategies and objectives.*"

The definitions above articulates ITG in relation to corporate governance and the importance of IT in the information age, of which IT is a vital component (Raghuphati, 2007). With organisations more reliant on information as an asset and its dependency on IT, they should also be cautious of the potential

threats such dependencies brings to the organisation, therefore it is incumbent on the organisation to ensure effective implementation of ITG.

IT provides organisations with a myriad of opportunities to gain advantage over competitors, enhancing operational efficiencies, through increased productivity, accuracy and processing of transactions (Boynton et al., 1994; Rockart al., 1996; Ross et al., 1996; Broadbent and Weill, 1997; Sambamurthy and Zmud, 1999; and Abu-Musa, 2006). Given the advantages that IT presents, there are a myriad of risks and threats. These risks includes loss of assets, an increase in fraud, loss of data and theft thereof, business disruption (Warren et al., 1998; Gelinas et al., 1999; Beasley et al., 2000; Hermanson et al., 2000; Hadden et al., 2003 and Abu-Musa, 2006).

The benefits therefore associated with ITG, is that the organisation is able to take full advantage of its information as an asset, gaining a competitive advantage and capitalising opportunities (Gaynor, 2002). Brown and Nasuti, (2005) and Symons (2005) confirm ITG outlines how and by whom business decisions are made, stressing accountability and the resulting outcomes are measured and monitored. Although Petersen (2004) acknowledges that ITG is complex, involving all affected stakeholders with varied views, goals and motivations, which silo view, will affect governance, Kakabase (2001) argued that ITG addressed business objectives that are widely impacted by IT.

According to Lainhart (2001) ITG is similar to corporate governance. IT is governed by best practises that ensure IT resources are utilised optimally and what it is intended for, risks are managed and business objectives are supported.

ITG therefore integrates best practice such as planning and organising, acquisition and implementing, delivery and support and monitoring of IT performance; ensuring organisational resources are utilised responsibly, risks are management and the technology supports the business objectives. Another vital component of corporate governance is ISG, as highlighted by Warren et al., 1998; Gelinas et al., 1999; Beasley et al., 2000; Hermanson et al., 2000; Hadden et al., 2003 and Abu-Musa, 2006 above; the increased usage of IT, increases the organisation risks and threats, therefore the protection of information as an asset is critical; ensuring protection of this resource.

2.3.3 Information Security Governance

ISG is defined as an essential component of corporate governance, ensuring management's commitment in achieving superior IS, enforced through appropriate organisational structures, appropriate policies and procedures, processes, technologies and compliance mechanism, ultimately ensuring the integrity, confidentiality and availability or organisational assets (Von Solms, 2006). IS should not be regarded as a technical matter (Dodds & Hague, 2004), but as a critical component of corporate governance, which is a management responsibility to ensure enforcement and compliance (Von Solms, 2005). This implies that all components of the organisation, from the board of directors, executive management to the lowest level employee has critical role to ensure compliance with appropriate policies and procedures to ensure the protection of the organisations information.

Adherence to ISG would yield the following benefits for the organisation:

- ISG will demonstrate due diligence (Moulton & Coles, 2003 and Von Solms and Von Solms, 2006), will have adverse consequences for members of the board of directors and managers of organisations, as they will be held accountable should they fail to implement appropriate mechanisms to protect information as an asset (King III, 2010).
- Increased organisational trusts, with increased IS (Corporate Governance Task force, 2004) leading to increased productivity and highlighted with ITG above, the organisation is able to take full advantage of its information as an asset, gaining a competitive advantage and capitalising opportunities (Gaynor, 2002).
- Von Solms (2006) highlighted that IS has progressed through four waves. Where initially IS was very technically inclined, it has progressed to a strategic imperative and an established component of corporate governance, which must be protected appropriately.
- ISG will ensure an increase in business value and increase shareholder satisfaction (Eloff, 1993; et. al Posthumus & Von Solms, 2004).
- Lack of ISG could lead to reputational deficit and potential decrease in revenue (Entrust, 2004).
- ISG will ensure adherence with legislation (Enstrust, 2004).

ISG as a critical component of corporate governance will ensure organisational adherence to internal control mechanisms and compliance with external legislation, regulations and policies, it is therefore incumbent upon the board of directors and management of the organisation to ensure such mechanisms and or instruments are implemented. Furthermore the advent of King III (2010), Code of Corporate Governance it would be crucial for the researcher to determine the impact of this instrument and highlight the relevance to the research, compliance with MISS by senior managers in the public service.

2.3.4 King III

IS has become integral to corporate governance and managing IT within organisations, thus ISG is key to compliance with the Code of Corporate Governance. This can be understood as organisations globally are making using IT tools more widely (von Solms, 2006).

A study conducted by Dagada, Eloff and Venter (2009) found that most organisations and government departments are in conflict with the spirit of good governance and do not take IS seriously. Many organisations have IS policies in place; however these were purchased off-the-shelve to ensure compliance with ISO2700 standards, and to gain certification. Dagada, Eloff and Venter (2009) states, a legal expert have observed that *"The problem is that very few IT security experts and practitioners are conscious about IS legislation. Technology people are more familiar with standards; unfortunately there is a myriad of legislation and governance internationally and in SA."*

The King II and draft III prescribe that the responsibility of IS rests with the company board of directors, which is often passed down to the CIO. In the spirit of good corporate governance the King III (2010) states, "*The board should ensure that IT is aligned with business objectives and sustainability*," meaning the board of directors would take direct responsibility for driving IS within an organisation. They will ensure the effective and efficient management of information resources, which includes people, funding and information.

The need to conform to international standards, namely BS7799-1, which is recognised by the draft King III, consists of three key components, namely integrity, confidentiality and availability of information.

In the following section the researcher will review standardization and international practices related to IS that will assist public service with enforcing good security practices.

2.4 Standardization and international best practices

Standardization will ensure that a common criterion exists throughout the public service ensuring that security is in place. It has become globally accepted that standards are a means to enforce good security practices. The adoption and compliance to attain certification of an international best practice will assist with organisational competitiveness and the public service would make a statement of its ability to manage IS.

According to Zuckermann (1997) there are two kinds of organisations that exist globally, those who have embraced internal standards and those with the intent too. Evidence have emerged that the adoption and compliance with international standards, is central to the development of countries competiveness. Globally there has been a realisation that information is the impetus of economies, which is dependent on the secure flow, both within and outside of governments, across businesses, there information security is of critical importance, ensuring such transactions or exchanges are conducted with the utmost integrity.

For a number of decades institutions have been working to establish high quality standards. The BSI has carried out studies for the purpose of establishing effective and high quality standards for this industry (BSI, 2004). During 1990s BS7799 has been responsive to the request of industry, government and business for the creation of a common IS structure. Through collective efforts by the USA, Canada, UK, France, Netherlands and Germany, the alignment began to ensure a single set of IS criteria was created for wide use, named Common Criteria Project.

During 1995, the BS7799 standard was opted by the UK Government. During May 1999 a 2nd version of BS799 was published incorporating significant improvements from its earlier version. This attracted the attention and interest

from ISO, who subsequently participated in the process of formulating this standard.

During December 2000 ISO took over BS7799 and it was re-branded as ISO 17799 and during September 2002 the 2nd part of the BS7799 standard was revised to ensure consistency with other management standards such as ISO9001:2000 and ISO140001:1996. This move towards alignment on international norms and gaining extended acceptance in the industry was significant.

IS with related supporting processes, networks and systems are important business assets, as the confidentiality, integrity and availability of information are factors contributing to the ensure the organisation maintains its competitive edge, cash flow, commercial image, legal compliance and profitability. The utilisation of tools such as the internet in the information age, has made institutions vulnerable to a range of security related threats, which have become more common and sophisticated (ISO/IEC 17799: viii).

The increased dependence on tools, such as information systems have made institutions both public and private more vulnerable, which is attributed to sharing of information resources and interconnected public and private networks (ISO/IEC 17799:viii).

The Conformity Assessment Organisation has processes in place to certify organisations who have implemented ISM systems, inclusive of ICT against a set standard. Commonly known as ISO/IEC 17799: 2000 Information Technology – Code of Practice for ISM aligns organisations practical frameworks and guidelines to bring about improvement in the management of IS, which has been adopted globally as a recognised international benchmark of effective ISM (SABS, 2002).

2.4.1 BSI & ISO

The public service is inherently dependant on the confidentiality, availability and integrity of information (ISO/IEC 17799: viii) to deliver a service to the citizens of South Africa. This information should be seen as an asset, with considerable value and has to be protected at all costs. IS protects these assets, from a range of threats to ensure continuity in services. This will be

achieved through the implementation of a range of processes, policies, procedures and controls.

The information systems and networks of the public service are faced with security threats from a wide range of sources, which include cyber crime, that is computer assisted fraud, espionage and sabotage. These sources of damage such as viruses, hacking, and phishing have become increasingly sophisticated as cybercrime has become economically viable.

Certification creates access to global markets, protection of patents and the environment, government acquisition reforms and improves quality (Howie, 1995). This is further confirmed by Solms (2001) where he states that an organisations increased dependency on technology, increases its vulnerability and costs with positive spin-offs as the creation of new opportunities.

Individuals who handle this information play an important role and their behaviour towards IS will determine the level of risk and exposure. Behaviour and perception toward IS can be improved through continued awareness and training (Caralli and Wilson, 2003).

Standardisation of IS policy controls and procedures are proposed, ensuring adherence to corporate governance and international security standards enhancing organisational resilience and improving its competency in protecting its information asset.

2.4.1.1 BS7799 – ISO17799/ISO25001 Security Standards

Information is considered an asset and invaluable to any organisation. Protection of information as an asset is critical to preserve the integrity and survival of the entity. Thus mitigation against risks threatening the security of this asset has to occur on a continuous basis and controlled.

According to GASSP (1995) IS is a combination of preventative, detective and recovery measures. The adoption of best practice will ensure that appropriate IS measures are in place and the best practice can be used as a yardstick for benchmarking when implementing.

ISO/IEC11779 is a code of practice for IS management, which is a guide containing advice and recommendations to supplement the initiation, implementation and maintenance of IS projects in an organisation. The objective is to ensure the security of or organisation's information according

the ten fields of application which is the underlying framework of security management.

ISO published ISO/IEC 17799:2000, IT – Code of Practice for IS during the late 2000's. The objective of ISO/IEC117799:200 are to enable business enterprises to mitigate those IT threats that arise from physical disaster, fraud and industrial espionage.

The ten fields of application of the ISO17799 Standards (ISO/IEC17799) are presented in the form of guidelines and recommendations, containing 36 security objectives and 127 security controls. Below is brief overview of the 10 fields:

Security Policy provides guidelines and management advice for improving IS. The formalisation of IS practices as established and approved by the top management for implementation and compliance by all stakeholders in order to protect the organisations assets.

Organisational Security is the management structure for security including appointment of qualified personnel, defining and assigning of roles and responsibilities as well as the establishment of process flows and controls for security management. In essence it facilitates IS management within the organisation.

Asset Classification and Control is a process of carrying out and inventory and assessment of the organisations information assets, which is inclusive of its infrastructure so that assets are secure, managed and controlled effectively.

Personnel Security minimizes the risk of human error, theft, fraud or abusive use of equipment by setting security expectations in job responsibilities. Through screening new personnel for criminal records, setting up confidentially agreements and reporting incidents are key elements covered under this field.

Physical and Environmental Security is measures that prevent the violation, deterioration or disruption of industrial facilities and data. Policies are established for the protection of infrastructure, plant and personnel.

Communications and Operations Management ensures adequate and reliable operation of information processing devices exists within the organisation using various preventative measures.

Access Control is the underlying structure for securing information using access controls to network, systems and application resources.

Systems Development and Maintenance ensures that security is incorporated into information systems and that security forms an integral part of any network and systems expansions. It further ensures that systems can be maintained over time.

Business Continuity Management focuses on planning activities for disaster recovery. It aims to minimize the impact of business interruptions and protect the organisations essential processes from failure and major disasters.

Compliance with regulatory frameworks to avoid a breach of criminal or civil law, statutory or contractual requirements and of security requirements are key elements of this element.

2.4.1.2 Benefits of BS7799/ISO17799/ISO27001 Standards

Compliance with BS7799/ISO17799 Standards brings about benefits for the organisations for consideration:

The Organisational Level

By attaining certification the organisation demonstrates its level of commitment towards securing its assets and information. Complying with such standards, the organisation gives a strong signal to stakeholders that significant efforts are being put in place to secure the environment, thus in essence protecting the interests of the shareholder.

Legal Level

The organisation has an obligation to comply with prevailing regulatory and legal frameworks. This is a direct demonstration to authorities that the organisation is fulfilling its mandatory duty by observing, respecting and complying with applicable laws.

Operating Level

The implementation of ISO27001 Standards elevates the operating conditions of any organisation, thus allowing the organisation to understand the operations from various perspectives and gain knowledge of information systems, its weaknesses and mechanisms of protecting it. The risks are better managed and possible threats minimised or eliminated.

Commercial Level

Organisations strive for differentiation from their competitors and have been identified as a critical success factor for business growth. Certification of BS7799/ISO17799 is methods utilised for differentiation and showcasing excellence, which reassure stakeholders about the organisational capability. The positive spin-off is that this raises stakeholder confidence levels, reassures trust and could lead to business growth.

Human Level

Whilst employees will grow their knowledge, inculcate best practice and disciplines in areas of IS. Employees will become more aware of security problems, threats as well as their roles and responsibilities to ensure the environment is secured. A security conscious culture is developed throughout the organisation.

2.4.2 Factors affecting ISM

Security objectives and activities must be conducted based on business objectives and requirements, led by the business management (Von Solms, 1998). The following factors should be considered during ISM implementation: people, culture, attitude, security education and training, ownership and responsibility (Nosworthy, 2000).

Managerial factors include top management support and commitment, security education and training and regulations. Additional critical factors are awareness and financial resources (Chang & Ho, 2006; Kankanhlli et al. 2003). This was extensively discussed in the aspects covering corporate governance, ITG and ISG.

Information Security Awareness

Humans are perceived as the weakest link in the IS environment. Employees should be trained about relevant policy requirements to ensure that there is no compromise of information, rendering the institution vulnerable to possible intrusion (Stephanou & Dagada, 2008 et. al Scheiner, 2000; Stanton et. al 2003:1 Katsikas, 2000: 130; Van Niekerk & von Solms, 2004:2; von Solms, 2000:618).

User has been involved with security awareness initiatives for a while (Wilson and Hash, 2003; Furnell and Phyo, 2003), but lately the security community encourages security officers to concentrate on security awareness initiatives, instead of investing in the latest "new security gadget". Barrett (2006) says an organisations need for the latest security gadgetry will be reduced through empowering people with appropriate awareness training, alerting them to the associated risks. The strength of organisational cyber-defence is a knowledgeable workforce.

IS awareness can be defined as the degree or extent to which every member of staff understands the importance of security, the levels of IS appropriate to the organisation and their individual security responsibility (European Security Forum, 1991). This definition clearly highlights that information and people are two critical resources that go hand in hand and security awareness is a people issue. The purpose of security awareness is to promote and maintain an environment that is positive to security, thus allowing staff to apply their minds and act proactively thus minimizing the vulnerability of the organisation against possible threats. The process is ongoing so that security awareness becomes a culture entrenched in the organisation and continuously direct peoples behaviour. This can be achieved through the training of employees. Training can be conducted using various methods within or out of the classroom. In order to sustain its effectiveness this needs to be refreshed on a regular basis to ensure the impetus is not lost. Intermittent campaigns to

ensure awareness of pending threats will ensure heightened awareness of employees. This will ensure they are regularly updated of threats eminent within the security scene.

IS awareness programmes has both short term and long term benefits for the organisation, as it will ensure the number of incidents are reduced in both number and scale, thus promoting the best practice. As every intrusion or incident has a cost associated, some are measurable and others not, however the impact of a breach in security will ultimately affect the organisation. The impact could be felt in recovery cost, meaning the organisation was unable to render a service, as this service was down for a particular period of time affecting the overall performance of the organisation. It also increases the confidence of customers and shareholders in the organisation, as they would deem the organisation able to render a good quality product or service. The organisation would have an assurance of business continuity. In the event of services affected, as the organisations do have business continuity plans, it would be able to ensure that services are continued, no matter what the location. The organisation is able to provide information of high quality for decision making and reporting purposes and confidential information is protected from unauthorised access by both internal and external individuals, competitors and thieves. In addition it will ensure that the organisation complies with legislation as data is protected.

Siponen (2000) says that it is crucial for users to understand policies, eliminating misinterpretation and misuse. However the message communicated to users is not beyond doubt very clear, as many of these situations perpetrated are complex and dynamic (Guant, 2000:152 – 153). According to Srikwan & Jakobsson (2007), identity theft is complex and the expectation from the user has to be communicated very clearly. On daily basis banks disseminate information to their clientele alerting them of potential criminals and incidents that they need to be cautious of. Individuals still fall prey to such criminal acts. This brings to mind the effectiveness of messages conveyed and whether individuals really pay attention to such information when distributed. Education of employees remains a necessity and managers would still have to ensure that they remain motivated to keep them abreast of the latest developments.

According to Danchev (2003) IS awareness is critical to ensure full compliance with your organisation's IS policy. This can be attained through engaging employees, allowing them the opportunity to actively participate in the protection of information as an asset.

IS is not a technical problem but a management issue. In recent years cyber attacks on governments, be it through email or web attacks, insiders have been sensationalised. South Africa has not been immune from these events. For example in 2003, a hacker named r00t3rs have maliciously destroyed co.za website (Malan, 2003). People play an integral part in the success of any security strategy. As they are responsible for handling information on a daily basis, their level of awareness is key. Security should be integral to their daily activities and this should be entrenched in the organisational culture. As these individuals have access to classified information, databases and networks, the organisation should ensure that it has policies and controls in place that will guide their behaviour. Surveys conducted by Ernst and Young Consulting (Ernst and Young, 2004) suggest that levels of awareness for both senior managers and personnel are cause for concern. By conducting these surveys on a regular basis the organisation would gain insight where training is required.

Information and communication technologies have presented the public service with a myriad of challenges, thus it is proposed the higher the levels of awareness against IS threats in the public service the lower the risks of potential threats against its information.

Key findings from the 2004 CSI/FBI Computer Crime and Security Survey highlighted that most organisations allocate between 1% and 5% of their IT budget to security, this function is not outsourced as 60% of respondents indicated that they perform this function themselves and most computer security practitioners think their organisations do not spend enough on conducting security awareness training for employees. When the question was posed to security practitioners what area they believe is most important to provide training, 70% of the respondents indicated security awareness training in the areas related to their security policy.

In the following section the researcher will review relevant legislation applicable to IS to ensure the preservation and protection of data.

2.5 Legislation related of Information Security in public sector

The advent of the information society and knowledge economy have added further complexities and diversity; with the utilisation of convergence in multimedia technologies; producing unlimited opportunities and challenges in the form of cyber activity. The utilisations of technologies have made the state vulnerable to cyber threats, thus the need to secure the country's information is a matter of national importance.

The researcher have reviewed various pieces of legislation, such as the Public Service Act, Intellectual property law act, Copyright Act, ECT Act and the MISS policy, to determine provisions contained within legislation that will ensure what the public service have to comply with that will aid in minimizing the risks and vulnerability of government information.

2.5.1 Public Service Act of 1994 and Regulations

The Minister for Public Service and Administration has been entrusted with the responsibility that relates to *any policy which relates to information management and IT in the public service*. In addition this incumbent *has to provide a framework of norms and standards with a view to giving effect to any such policy and draft regulations in terms of the Public Service Act.* With the increased usage of technology and information being transmitted over various mediums, it is critical that the Minister ensures IS is enforced and there are clearly defined policies and guidelines, which will ensure a secure environment exists for usages of such media.

The Public Service Regulations of 2001 which emanates from Section 41(1)(d)(iii) of the Public Service Act of 1994 makes provision for employee compliance to ensure the safeguarding and integrity of information. The regulations stipulate that *employees may not release official information unless the necessary authority has been granted.* Key in facilitating compliance is the awareness of individuals accessing this information, be it in the form of transacting, capturing, processing or extracting for reports.

Departmental heads are charged with the responsibility to ensure that an Information plan is supported by an IT plan enabled by a operational plan.

This will ensure information is managed in a secure environment. It further gives credence to the usage of IT to promote efficiency, effectiveness to improve the management and functioning of departments.

2.5.2 Copyright and intellectual property

The Intellectual Property Law Amendment Act of 1997 and Copyright Act of 1978 provide a framework for the establishment, protection, registration, maintenance, management and use of ICT Intellectual Property. This legislation is applicable to all employees, third parties, external contractors and ICT Intellectual organisations. Over time intellectual property has become an important asset. This includes assets such as software developed, domain names, websites and its source code. When employees copy or distribute intellectual property without the permission of the rightful owner or purchasing of appropriate licenses the individual is in contravention of legislation.

2.5.3 Electronic Communications and Transaction Act of 2002

Cybercrime in the ECT Act, Section 85 is defined as when a person becomes aware that they have access to data which they should not have, but continues to access the data illegally. This legislation further makes provision for the legal recourse that can be taken, when such instances are detected. Section 86 (4) further states that a person who uses a computer or any other devise to illegally access data to overcome security measures that protects information are guilty of committing cybercrime. Furthermore Section 86 (5) states that a person who commits an act to interfere with access to information that results in denial of access to authorised users are guilty of committing a criminal offence.

2.5.4 Minimum Information Security Standards

The objective of the MISS is to provide procedures and measures to protect information that will impact the vulnerability of state should it be compromised by any means. This standard also addresses aspects of the responsible head of the institution, physical, personal and computer security that compels the three spheres of government, namely national, provincial and local government, parastatals and state owned enterprises of a minimal standard of adherence.

The institutional head will be accountable and ensure the provision and maintenance of security at the institution. (Chapter 3, pg18) Although he has

the power to delegate this responsibility he has to ensure that security personnel are employed, provide training and exercise control, manage and administer security, namely planning, organising, financing, staffing, guiding and controlling.

Chapter 5 address guidelines to security vetting of personnel. All personnel from the lowest level to that of deputy-directors general must be subjected to security vetting. The level of clearance adjudicate to a person is determined by the type of content the person requires access to and this is subject to the need-to-know principle.

Physical security measures entail access control, key control and combination locks. To achieve an optimal IS environment, system security measures are essential. There are key prerequisites that will determine the effectiveness of security and this is further impacted by the weakest link. Effective key control will be ensured by keeping effective records to ensure that keys used to access classified information are dealt with in a controlled manner.

Communication security is regarded as part of the MISS. It may be described as a condition that is created by the application of measures to safeguard sensitive communication in any form. This standard document addresses storage of such information and it compels departments to implement measures that will ensure the back-up of essential information, allocation and use of passwords, physical security measures as prescribed and the establishment of security responsibilities.

Employees in the public service plays a key role insuring the effectiveness of MISS, it is thus proposed the higher the levels compliance of awareness of the roles and responsibilities related to MISS, the more information will be security, with less vulnerabilities and less risk associated for the public service.

2.6 Information Security Management

The complex nature of IS management requires that it is managed in a holistic approach by the leadership of that organisation. The challenge for achieving general goals of IS are the safeguarding of sensitive information, protection of the systems that host the information from potential loss, damage or destruction, providing assurances that the integrity, availability and confidentiality is not tainted, compliance, enforcement of legislation and regulatory frameworks to ensure the latter (Hong et al., Tudor, 2001). In the case of the public service for SA, MISS makes provision for the protection of information as an asset to minimise the vulnerability of the state. This is perpetuated as the public service is inherently dependant on the availability of information to deliver a service to citizens of SA. For example during May of 2004, a total of 25 government departments were hit by the Sasser virus, with the main network shutting down (Sepotokele, 2004). This had severe implications for the country as the government departments affected were unable to access pertinent information. One example of such systems that were affected was that of hospitals, as patient records are online and scheduling of operations is automated. This resulted in delayed operations and hospitals reverting to a manual system to ensure scheduled patients could be attended to.

The protection of information should be entrenched in an organisations' strategic objectives; and it is pertinent for the leadership to realise that the safekeeping of this asset is not just a technical aspect, but a business imperative (Solms and Solms, 2004). IS should not be viewed in isolation but holistically, taking into account the following elements, namely environment, legislation, personnel, technology, compliance and ethical considerations.

Ngobeni & Grobler (2009) further affirms that the implementation of appropriate policy and enforcement of the latter will enable the protection; preservation of such information as an asset, which is the cornerstone of effectiveness. Without an IS policy a government department would not have a baseline to determine a consistent manner to control and monitor its environment, which would lead to inconsistencies and leave the department vulnerable to potential threats and intrusions by external parties.

2.6.1 Five Pillars of Information Security

According to authors Pfleeger, Steiner, Krause & Tipton (Krause & Tipton, 1999; Pfleeger, 2000) there are five pillars that make today's security techniques, namely Identification and Authentication, Authorisation, Confidentiality, Integrity and Non-repudiation, which has been defined in ISO7498-2 standard as produced by International Standard Organisation (ISO, 1999).

2.6.1.1 Identification & Authentication

Identification is the process of issuing and verifying those access privileges, thus certifying the individual is able to perform certain activities. Authentication is a means of verifying authenticity to determine whether an individual is saying who they are. There are 3 basic ways whereby people are able to authenticate themselves, something they know (passwords), something they have (card) and something they are (biometric data, such as fingerprints). These methods have their own strengths and weaknesses, thus it is recommendable that 2 or 3 methods are utilised simultaneously, which is called a two-factor authentication.

2.6.1.2 Authorisation

This refers to the privileges and permission granted, to a person by the delegated responsible party to access a system, information or program. Such privileges are often granted on a need-to-know basis. Persons holding such authorisation are commonly known as the authorised person and they have the responsibility to ensure that such privileges and permissions are not disclosed to other individuals not authorised.

2.6.1.3 Confidentiality

Confidentiality means keeping information from being seen by others who are not authorised. It refers to how data is collected, used and maintained within any organisation. This does not preclude the protection of data from passive attacks and requires that only authorised personnel has access to information.

2.6.1.4 Integrity

Ensures that data is a proper representation of information, accurate and in an unimpaired condition, meaning keeping information from changed unauthorised. Measures should be put in place to ensure that data is

protected from intentional or accidental alteration and exposed to accidental or intentional destruction.

Confidentiality and integrity are important when information travels by means of the internet, as this is defined as a public space and interception is possible thus making the information vulnerable, which can be countered through the utilisation of encryption tools to counter such threats.

2.6.1.5 Non-Repudiation

It eliminates denial by either, the sender or receiver, that a transaction or communication of sensitive information took place. This service proofs that someone was the actual sender and who the receiver was, furthermore it can confirm whether or not an imposter was involved either side. According to Schneiner (2000), these services are imperative to ensure information is protected and secured during storage, transmission and usage.

2.6.2 Information security related crime

Computer crime cannot be defined by a single, clear definition as we would be unable to cover all the aspects that relates to computer crime (Wallace, Lusthaus & Kim, 2005). It is for this reason that we can define computer crime as the contravention of any criminal law that required the knowledge or use of computer or computer aided technology in its perpetration, investigation or prosecution (Goodman, 2001). Computer equipment can also be the target of the offence and not just the tool to committing the crime (Nceba, 1999). These crimes are committed by perpetrators who have the intention to gain unauthorised access to tangible assets, such as goods, materials, money and decision making information. Primarily they intend to manipulate salaries, invoices, social security payments, account balances and pensions (Sieber, 1986).

2.6.2.1 Cyber crime

Cybercrime can be defined as any criminal activity through the use of a computer, network or hardware device to perpetrate a crime (Symantec, 2008). Unlawful online activity is commonly referred to as cyber crime. Law enforcement agencies became aware of this criminal activity during the early 1990's, once the internet became an accessible facility connecting business to

the outside world and was utilised as a platform for trading and an increased dependency as a business tool.

During 2001 the United Nation General Assembly adopted a resolution on Combating the Criminal Misuse of Information Technologies. This was a call to all member states to become aware and prepare necessary legal and administrative procedures to prevent and prosecute cybercrime (Pipe, 2003).

There are various types of cybercrime such as hacking, viruses, computer espionage, identity theft, e-mail crimes and violation, social engineering and insider threats which will be discussed in more detail below.

2.6.2.2 Hacking

Hacking is considered a crime when computers and associated networks are used unauthorised, with the intent to commit a serious offence and changes are affected to data with the intent to inconvenience the hacked party or parties (Krone, 2005).

Hackers can be defined as an illegal intruder, former employee or a third party connection, which uses an arsenal of techniques to access valuable company information. The hacker of today circumvent network security by disguising themselves as legitimate users, facilitating legitimate access by intruding and infiltrating systems to gain access to critical company data, such intellectual property, financial information or personal customer information (Bingham, 2005). By gaining access through a legitimate account the hacker can access systems without breaking down security gates, but accessing systems with legitimate credentials they gather along the way. These credentials are stolen in a variety of ways, either by tricking employees into divulging passwords, user names or sniffing an ISP. A matter of key concern is that many organisations do not have the means to detect these compromises. These are only discovered when information is already in the public domain.

The main objective of a hacker is to cause destruction, through the release of virus worms, Trojan horses, propagation of malware and spyware, DoS attacks, spam, phishing campaigns and social engineering exploits on unsuspecting human targets. Hackers pose grave risks to both private citizen and businesses; and for this reason many organisations have gone to great

extents to protect and secure sensitive computing systems against such external threats (Steele and Wargo, 2007).

2.6.2.3 Viruses

A computer virus can be defined as self replicating, self executing program written to maliciously change the functioning of the computer, without the consent of the user (Gordon, Loeb, Lucyshyn & Richardson, 2005). Virus code distributions are made easier by the increased usage of internet and e-mail as part of our daily communication (Coulthard & Vuori, 2002).

Interestingly viruses are not harmful by nature, but this is dependant on the additional elements contained within its code. Some have annoying effects on the computers they infect, whilst others have caused widespread damage (Jones, 2007).

Worms are standalone programmes that are able to replicate itself over a network without any action by the user. Like viruses, worms are destructive in nature, should this be written in its code. Examples of such programmes are the “ILoveYou bug” which spread faster than the “Melissa” virus. The infection spread to millions of computers, and caused corporations such as Ford Motor Company to shut down its e-mail systems. These programmes were also able to reach CIA, NASA and DoD in the USA (Jones, 2007).

A Trojan horse is another form of virus, that appears to perform a useful function, however contains a hidden malicious code. It either acts as a delivery vehicle or permits unauthorised access by another. It often contains spying software or “backdoor” functions that allow a remote user to gain information about the computer or actually control the computer via the network, creating a “zombie computer,” (Jones, 2007).

A DoS is the unauthorised disruption of website with network traffic and disrupts their ability to communicate with legitimate users. These attacks commences when an individual obtains unauthorised access to a computer system and places software code on it that renders that system a master. The individual also breaks into other networks to place a code that turns those systems into agents, commonly known as zombies or slaves. Acting in unison the agents generate a high volume of traffic from several sources, rendering

the destination computer overwhelmed and it loses its ability to serve legitimate customers (Jones, 2007).

2.6.2.4 Computer espionage

Computer espionage activities involve the use of organizational information systems by insiders for the retrieval of data, which is stolen and sold to others, to the detriment of the organization (Band et al., 2006). Sabotage is the destruction of data and information systems (Cappelli et al., 2006). These criminal activities may be committed for various reasons, namely retribution, dismissal, substance abuse or as a means to earn additional income to alleviate financial debt (Knapp *et al.*, 2006; Giacalone, 1987).

Computer espionage can be defined as the act or practice of spying or using spies to obtain secret information about government or business competitors. Information can be obtained by employing two methods, namely human intelligence and or technical intelligence (Biesterfeld, 2008). In order for this operation to be successful the collector will gain access to individuals who will collect the information or the placement of a collector to ensure the relevant information is obtained. To ensure this takes place it is critical to identify the correct resource to obtain the necessary information, who has access. This individual will be concerned with the copying of data files, corruption or extortion of employees, infiltration of an organisation by employees from competitors or governments to obtain information. Perpetrators can also access, intercept and record “electronic fields” through radiation generated by computers (Sieber, 1986).

Espionage is sometimes sanctioned or carried out by foreign governments. Various countries who have earned a reputation, where this practice is acceptable are France, Soviet Union, China and Latin America (Kirkpatrick, 2008).

2.6.2.5 Identity theft

Identity theft occurs when a person uses knowingly without permission of another person, his/her identity to gain access to information, be it financial, medical or of their character (Federal Trade Commission, 2004). This can be with malicious intent or to gain access to information which they have no clearance for. The identity theft of today is a white-collar, computer-savvy

employee with desktop access to large databases that contains thousands of personal customer information, such as identity numbers, credit and bank account numbers (Fertell, 2003). It is estimated that half of all identity theft cases come from raiding business data banks as it is discovered that technology systems lacks proper safeguards and oversight to regulate unsolicited access. In the USA during 2001, 86 000 complaints of identity theft were received and this almost doubled a year later to 162 000 (Federal Trade Commission, 2002).

In the case of identity theft, the imposter steals or obtains key pieces of personal information to create a persona and commit various fraudulent activities resulting in personal financial gain at the expense of the victim. These crimes know no boundary and can be committed from anywhere in the world. Perpetrators employ various methods, either sophisticated or unsophisticated methods to gain access to your data. Access is gained through stealing company records or information, bribing an employee who has access to such records, hacking into company systems. These perpetrators would also go to extreme methods such as searching through your dustbins, stealing of post, “skimming” of debit and credit card information.

2.6.2.6 Insider Threats

Devastating cases of intentional information security breaches by trusted insiders occur on a regular basis (Herbig and Wiskoff, 2002). To safeguard the organisation’s integrity and brand, companies seldom report security breaches, as this will have devastating financial implications and questions around trust of the organisation. The ripple effect continues as case studies are lost, when such incidents are not reported, resulting in relatively little is known about the conditions, including our inability to properly profile perpetrators (Crawford and Bosshardt, 1993).

Insiders are a clear threat to information systems, namely intellectual property, thus it proves more and more difficult for organisations to prevent compromises by such individuals. They can be defined as individuals who have legitimate access to a company’s physical and computer systems; being current employees, contractors, vendors, suppliers, temporary visitors, former employees or retirees (Kirkpatrick, 2008). These individuals are aware of the

organisations vulnerabilities and how to take advantage of the vulnerabilities to meet their objectives. According to Bietersfeld et. al Kirkpatrick, “Although technical intelligence such as photography or eavesdropping reveal a great deal of information, people remain the best source of information.”

An empirical study in Germany confirmed that 90% of contraventions were committed by employees of companies affected. 60% of perpetrators who committed these crimes had no specialized computer or programming skills. It is not clear if the crimes of perpetrators with specialized skills are more difficult to detect, however the motive of perpetrators was purely for financial gain (Sieber, 1986). A study conducted by PWC during 2007 on the global state of information security estimated that 69% of database breaches were conducted by employees within the organisations (PWC et. al Aldhizer, 2007). Although insider attacks are not as prevalent as outside network attacks the effects can be more detrimental as insiders know exactly where to go and have the means to cause greater harm to internal networks and applications. According to Gartner in 2005, 84% of security breaches occur when employees send confidential information outside the company, without being detected by the sophisticated network security employed by the organisation, as these employees are authorised users with access to the information at hand.

The external intruder of yesterday is the trusted employee of today who has gone bad. These individuals are determined to go unnoticed of the existing security systems in order to achieve their goals. The attacks have become more sophisticated as cyber crime has become profit-driven and this is the major motivator in many instances (Ortega, 2006). Trusted employees who have access and authorisation to critical information cannot be contained when they become malicious, thus organisations has to adapt their approach in managing IS to ensure the protection of the information asset.

ERP that enhances B2B processes has made transacting easier, however the risk to organisations are also increased as all business processes that were manually conducted are now automated thus increasing the chances of theft of intellectual property, personal consumer data and financial information (Aldhizer, 2007). These newer technologies that facilitate information sharing, further increases the risks of abuse of critical data. Companies have invested

heavily in integrated systems; very few have acquired software that will detect internal breaches. It can be concluded that the risk associated to the organisation is within their risk-tolerance levels (Aldhizer, 2007). For example a mid-level IT manager at the Canadian Defense Department created bogus orders that were funnelled through a supplier to front companies from which he would get kickbacks. This is to illustrate that IT staff are not above reproach. There was also the disgruntled system administrator who installed a time bomb at UBS that took out 2000 servers while he bought shares. The reported cost amounted to $3.1 million however the effects of not being able to access systems at 400 branches were not reported (Steinnon, 2006).

There are various reasons why employees would pursue this line of action. Financial gain has been identified as a primary reason, but this is not the case in all instances, namely career setbacks, whereby employees who were not promoted or demoted for various reasons and possible future retrenchment thus wanting to embarrass the organisation publically. Nationalist reasons are also one of the reasons, a foreign nationalist have a sense of loyalty to their home country. Foreigners do not seek to harm the company however they want to assist their foreign counterparts get an advantage in the marketplace.

For ideological reasons insiders may act against the organisation they are employed in, to further their goals. For example in 2004 terrorists reportedly planned to poison the drinking water of a major USA city during the chlorinating process by recruiting insiders to work with them, according to the Associated Press, Kirkpatrick, 2008.

2.6.2.7 E-mail Crimes and Violations

E-mail crimes are not new and has aided with making violations more widespread. This is perpetuated, as with e-mail you are able to reach a wider audience and no corner of the globe is unreachable. Crimes that are commonly committed through this facility is fraud, by use of phishing e-mail; distribution of pornography, which is prohibited by many company policies.

Chain letters are also seen as a form of abuse, with the promise of reward, which is never realised. Authenticity of the e-mail cannot be verified as the original header is lost in re-transmission from one user to another.

Spamming is the distribution of unsolicited commercial e-mails. The perpetrators obtain the e-mail addresses through vulnerable servers and exploit these facilities for the distribution of large batches of e-mail. They hope to entice vulnerable users to open their e-mail, which could potentially cause harm to the user's machine, network or the intent to obtain personal information from the user for financial gain.

Harassment is another form of crime committed through e-mail. A common form is that of sexual harassment, where colleagues would distribute jokes with sexual content to each other, inevitably offending someone within the office environment.

The range of cybercrime is broad. The different categories are neither co-extensive nor mutually exclusive, thus a cybercriminal may choose to carry out a specific intrusion to gain access so that he may perpetrate the crime. Each of these crimes has the power to cause tremendous damage, whether economic loss or intangible harm, such as the distribution of pornography or access to personal data (Jones, 2007). In the section following the researcher would outline the conceptual framework followed.

2.7 Conceptual Framework

The purpose of this research is to investigate factors of non-compliance of ISM in the public service of South Africa. The researcher would then present the findings and interpret and analyse findings on the management of IS.

In order to fulfil the objectives of the research, the researcher had to develop a conceptual framework, which is described a broad set of ideas and principles from ISM, which was used to structure the presentation of the research report (Reichel & Ramey, 1987). The conceptual framework is a tool that develops awareness and understanding of the relevant field of enquiry, in this case ISM. According to Guba and Lincoln (1989) the conceptual framework is an agenda of negotiation.

As in the case of this research of investigating factors of non-compliance of ISM in the public sector of South Africa, the researcher was able to explore corporate governance, IT Governance, ISG, international IS standards; South African legislation and definitions applicable to ISM to determine the impact on factors of non-compliance. In the past information security was assigned to

the IT Manager, however there has been paradox and it now widely acceptable that all in the employ of the public service, management and staff should contribute to compliance with information security policy. With the acceptance of the Codes of Good Practice, King III Report, Members of the Board of Directors, CEOs and Managers at a strategic level are held accountable for the implementation of IS and executing of oversight responsibility in respect of governance to ensure compliance. These shifts are attributed to global developments in corporate governance and organisational acceptance of IS accountability.

A study conducted by Dagada, Eloff and Venter (2009) found that most organisations and government departments are in conflict with the spirit of good governance and do not take IS seriously, informed the development of the framework, the research design and the means of investigating the realities of the current situation (Smyth, 2002).

Goetz & LeCompte (1984) stated that a conceptual framework, assist the researcher with a roadmap to ensure the research process remains on track through:

- Present linkages between the literature and the research objectives;
- Present reference points of literature, methodology and analysis of data;
- Inform the research design; and
- Assure trustworthiness of the study.

The objective of the conceptual framework is to provide the researcher with a roadmap, the researcher should be aware of the limitations of this concept as highlighted by Mason & Waywood (1996). The framework limits the results of the investigation, as there is a myriad of data available and impossible to consider all in one study. The frameworks construction is bound by the experience of the researcher and the sensitivity to certain occurrences are either consciously or unconsciously increased. Whereas Miles & Huberman (1994) advises the researcher to remain open to new and unexpected occurrences when reviewing data in the investigation process.

2.8 Conclusion

For the purposes of clarity the researcher gained an understanding of what a literature review entails, to ensure that all components are met and remaining within the confines and prescriptions of conducting research that is scientifically reliable and acceptable.

The literature review was divided into four sections and as outlined in the conceptual framework this approach was followed to ensure the appropriate linkages with research objectives are highlighted, present reference points of literature, methodology and analysis of data, which informed the research design.

Therefore the researcher reviewed literature related to role of governance in ISM, looking at corporate governance, ITG, ISG and the King III report on good governance, to highlight the relevance of these methodologies to ensure compliance and the role of the board of directors and executive management to ensure such policies and directives are implemented with the view to protect the organisations information, as it is an asset that impacts the integrity, reputation and drives organisational competitiveness.

The second section the researcher reviewed literature related to standardization and international best practice, to gain an understanding of the common criterion that exists, ensuring that IS is in place. The researcher has found that standards related IS has gained acceptance globally and are a means to enforce good security practices. The adoption and compliance to attain certification of an international best practice, drives organisational competitiveness and the public service would make a statement of its ability to manage IS to ensure the integrity and confidentiality of citizen data.

The third section the researcher reviewed literature related to legislation and policy instrument, namely MISS that applies to the South African context. It was established that various pieces of legislation, such as the Public Service Act, Intellectual property law act, Copyright Act, ECT Act and the MISS policy, to determine provisions contained within legislation that will ensure what the public service have to comply with that, will aid in minimizing the risks and

vulnerability of government information. The MISS clearly outlined the various responsibilities of management within public service to ensure such assets and data are protected.

The fourth and final section of the literature review, the researcher reviewed literature related to ISM and what is required from management to ensure IS is managed holistically. As highlighted by Solms and Solms (2004) the protection of information should be entrenched in an organisations' strategic objectives; and it is pertinent for the leadership to realise that the safekeeping of this asset is not just a technical aspect, but a business imperative. IS should not be viewed in isolation but holistically, taking into account the following elements, namely environment, legislation, personnel, technology, compliance and ethical considerations. Without an IS policy a government department would not have a baseline to determine in a consistent manner to control and monitor its environment, which would lead to inconsistencies and leave the department vulnerable to potential threats and intrusions by external parties.

Chapter 3 - Research Methodology

3.1 Introduction

The primary purpose of this research is to investigate factors of non-compliance of information security management in the public sector of South Africa.

In this chapter, the chosen methodology to address the research problem is described. This section of the document describes the approach and process for this study. In addition, the questionnaire design, the target population, the sampling and collection method, the data analysis tool and methodology are discussed. Finally validity and reliability of the chosen method of research are discussed.

Mandatory requirements for solving the research problem are the availability of correct data and research methodology used, as senior managers in the public service cannot take decisions based on perceptions, but decisions that are informed and supported by scientific methodologies (Mustafi & Roa, 2003). This implies that through appropriate data analysis, conclusive conclusions can be drawn, supported by facts.

The research was conducted in two phases, starting with the literature review, ending with summary and conclusions. The objective of the literature review was to present an overview of recent research on IS, as well as the influences of legislation and regulatory requirements, in relation to ISM. A substantial quantity and a variety of material was produced on the topics covered, such as IS standards, certification and governance forced the researcher to be selective in compiling the literature review. The subject of IS has evolved significantly and the researcher had to be mindful of the need to remain coherent, thus ensuring alignment with the purpose of the research.

The next step was the development of the survey in the form of a questionnaire. The content of the questionnaire focused on the compliance with MISS, thereafter selecting the sample size and population to participate in the questionnaire survey.

Phase two consisted of the collection and analysis of data, a statistical overview from which findings of the survey have been documented and concluded with the findings, conclusions and recommendations.

The methodology approach used will be discussed in the section following.

3.2 Research Methodology

Empirical study was applied to achieve the above research study. Research methods such as qualitative, quantitative and triangulation can be termed as empirical research (Goodwin, 2002).

A methodology is an organised way comprising of sequences, procedures and systems to manage and run research processes (Welman and Kruger, 2004). Welman and Kruger (2004) further states research involves the application of various methods and techniques in order to create scientifically obtained knowledge using objective methods.

A system consisting of various interrelated components needs to be employed and applied logically and sequentially, in order to generate and report confirmable findings about answers to a problem or scenario; hence the research chose this specific research method.

The method used by the researcher lay a pattern of soliciting applicable data, interpretation of data, drawing up a conclusion and reporting the findings (Olivier, 2004).

The researchers approach was to conduct an empirical research study which was quantitative in the form of a survey research design, and will be discussed in the next section.

3.3 Quantitative Research

Research methodology consists of methods, namely quantitative, qualitative and mixed methods. The researcher followed a methodology that focused on

the manner in which the research will be planned, structured and executed in order to comply with scientific criteria (Mouton and Marais, 1996).

Leedy and Ormrod (2005) further states that quantitative study resides broadly under the heading 'descriptive quantitative research.' This research involves identifying the characteristics of an observed phenomenon or exploring possible correlations among two or more phenomenon. Descriptive research examines the situation as it is, therefore it does not change or modify the situation under investigation, nor intend to determine the cause-and-effect relationship.

Research methodology forms an integral part of any research that will be undertaken (Leedy, 1993). Methodology will assist in explaining the nature of the data and the methods employed to generate appropriate conclusions. The researcher determined the process that would be appropriate for the research as the process would assist in answering the research questions (Crotty, 1998).

A descriptive study may be simple or complex, which can be done in various settings (Cooper and Schindler, 2003). Leedy and Ormrod (2005) states that descriptive research designs and approaches involve observation studies, correlation research, development designs and survey research. These approaches yield quantitative information which can be summarized through statistical analysis.

Quantitative researchers seek explanations and predictions that generalise to other persons and places (Leedy and Ormrod, 2005). The intention is to establish, confirm or validate relationships and to develop generalisations that contribute to theory. Quantitative studies represent a mainstream approach, structured guidelines exists, which should be followed carefully when conducting such research. Prior to commencing the study the researcher would have developed concepts, variables, hypothesis and methods of measurements, which would remain the same throughout the study. These methods are chosen, as it allows the quantitative researcher to remain objective when measuring the variables, detached from the research participants so that the researcher is able to draw unbiased conclusions (Leedy and Ormrod, 2005).

3.4 Research Approach

Quantitative research pertains to “cold” research that controls and manipulates variables (Leedy, 1993). It utilises numbers to describe characteristics of the unit of analysis and describes the relationship between variables. Theoretical explanations and concepts are important in the research design, as it represents the basis and interdependency of variables (Neuman, 2003).

Quantitative research has the following characteristics, namely a high level of formalisation and control, the range is defined in a more exact manner and it is relatively close to physical science (Mouton and Marais, 1996).

Probability sampling consists of simple random, systematic, stratified and cluster sampling. This research focussed on stratified sampling. According to Neuman (2006) the researcher will divide the population into strata. A random sample will be drawn from each stratum. It allows the researcher to control the size of each stratum, which will guarantee representation.

A quantitative approach will assist the researcher to investigate factors of non-compliance of information security management in the public sector of South Africa.

3.5 Research Design

A survey can be defined as a technique that is used to collect data from a sample population by means of a questionnaire (Zikmund, 1987). This instrument proved most useful as the researcher was trying to obtain information from respondents geographically based across SA in the public service (Leedy and Ormrod, 2005). Posted and e-mail surveys was not used to avoid a high non-responsive rate (Zikmund, 1987).

For this study the questionnaire was distributed at an annual function where senior managers across the public service were represented.

A quantitative approach was deemed the most appropriate method for conducting this research as statistical information would be able to investigate factors of non-compliance of information security management in the public sector of South Africa.

. The statistical information obtained will allow the researcher to generalise to the greater population from which the sample was drawn.

The researcher used probability stratified sampling, as this research randomly targeted managers at various job levels who have a responsibility and are directly involved with protecting information and ensure compliance with necessary policies, procedures and control of information.

The researcher developed a survey questionnaire that measured IS awareness, compliance with governance and international standard using the Likert scale based on a 1 to 5 rating (Likert et. al Neuman, 2006). The researcher distributed the survey questionnaire to the sample identified, by hand as the initial tool, namely Survey Monkey identified had various limitations. Using this approach presented the researcher with numerous advantages, namely:

- Survey research was easy to administer and manage;
- Maintaining confidentiality is of utmost importance and it afforded the respondents the opportunity to respond honestly with no fear of prejudice;
- Research ethics such as anonymity and the freedom to participate was not compromised.

Surveys are also efficient, inexpensive, accurate and quick (Zikmund, 1987). Survey questionnaires are not without disadvantages and the response rate could be poor and data could be biased, based on the participant's level of comprehension and understanding (Leedy and Ormrod, 2005). A survey also has the potential of limiting the respondent's opinions as it cannot be clarified (Cooper and Schindler, 1998).

3.6 Population and Sample

3.6.1 Population

A target population is a group that a researcher is interested in and on which the researcher wishes to draw conclusions (Kothari, 1985). For the purpose of this study, the population was defined as HOD's, CIO's, ICT Managers and Lines of Business Managers employed in the public service. This population is directly responsible for both compliance and social aspects of the IS management. A total of 100 surveys were distributed and a total of 100 surveys were returned. The sample size totalled 100 (n) respondents.

3.6.2 Sample and sampling method

Sampling is when the researcher utilises a small group of people that are representative of the population. This allows the researcher to make generalisations about the population it sampled, based on theories of probability (Neuman, 2006). The researcher used probability stratified sampling, targeting HOD's, CIO's, ICT Managers and Lines of Business Managers employed in the public service.

3.7 The research instrument

The research instrument chosen for this study was a questionnaire with 3 sections. The advantage of using a survey questionnaire for this study was that the researcher could pose close-ended questions which are related to the underlying factors under investigation (Zikmund, 1987). The questionnaire was structured as such that a covering letter outlining the purpose of the research and stressing to the respondents that confidentiality will be maintained (Kalof, Dan and Dietz, 2007).

3.8 Data Collection

The researcher collected both primary and secondary data for this research. Primary data was collected through a self designed survey questionnaire, distributed to a stratified sample of the target population. The survey method was selected as the researcher will be able to measure factors of non-compliance with the ISM of the sample and generalise it to the population (Neuman, 2006). The survey questionnaire was distributed by hand to senior managers of public service at an annual function, i.e. 100 survey questionnaires were handed out at this annual event. Prior to handing out the survey questionnaire permission was sought from the host to ensure that they are aware of the survey questionnaire and they also motivated senior managers to complete the questionnaire with announcements on arrival and at the tea break. This method ensured that the host was aware and prepared on what was required, should questions arise. Secondary data was obtained from books, journals, case studies and articles.

3.9 Data Analysis

Through quantitative analysis of the data obtained the researcher was able to analyse what is inside the data. The researcher manipulated and organised the quantitative data to reveal the truth about the research conducted (Neuman, 2006). Numbers are a representation of variables, which allows the researcher to measure the characteristics of subjects. The completed survey is a representation of data in a raw form. The researcher had to organise the data, so that it is readable by the computer which resulted in graphs and charts for interpretation by the researcher (Neuman, 2006).

Data analysis is the manipulation of quantitative data that allows the researcher to reveal matters of interest contained within the data about the population surveyed (Neuman, 2006).

After the researcher collected the data it was coded through the use of a code book. The raw data was translated into numbers which represented values of variables which measures the characteristics of the respondents, subjects and other cases suitable for computers.

3.9.1 Data Preparation and Description

In the research design stage or at least by the completion of the research proposal, the researcher had to decide how she would go about analysing the data (Cooper and Schindler, 2003). For the purposes of this research, the researcher made the decision on how to analyse the data during the design stage. Prior to analysing the data collected, the researcher embarked on developing a code book, which was utilised during the data entry and coding, prior to data analysis. According to Cooper and Schindler (2003), these activities ensure the accuracy of the data and their conversion from raw form to reduced and classified forms that are more appropriate for analysis.

In order to analyse the raw data from the questionnaire, the researcher edited the data for any errors and omissions to ensure that the responses were consistent with the intent of the survey questionnaire. The next step was to tabulate and code the raw data. Cooper and Schindler (2003:456) states that, coding involves assigning numbers or other symbols to answers so that the responses can be grouped into a limited number of classes or categories. To achieve this raw data from questions was entered into an EXCEL spreadsheet for tabulation, with each response given a code, as previously identified in the

code book. Most of the questions used the Likert scale, with responses ranging from Strongly agree to Strongly disagree, consisting of 5 categories within, the code range of 1 to 5 was allocated to each of the responses within the particular question.

The final step in the data preparation and descriptive process was the data entry. Data entry converts information gathered by secondary or primary methods to a medium for viewing and manipulation.

In addressing the research questions and the objectives, a quantitative research was used to obtain data. Data was collected through the means of distributing a survey questionnaire. The survey questionnaire constituted the most important and valuable source of information to address the hypotheses.

3.9.2 Coding of Data

Once the respondents completed the surveys, the researcher had to conduct a quantitative analysis of the data. This means that the researcher had to convert the data into numerical equivalents for the purposes of a quantitative analysis and statistical interpretation. The researcher cleaned the data for coding. Coding is when the researcher systematically reorganise raw data into a format that is readable by a machine (Neuman, 2006). This aided the researcher to be consistent with a representation of data, by applying the same rules throughout the analysis of the survey. A codebook assisted the researcher to predetermine the rules upfront. The researcher assigned numbers to a variable attribute (Neuman, 2006). The researcher assigned a number to each completed survey, thereafter capturing the data by creating a grid, of which each row represented a respondent and each column represented a variable.

The researcher had to be cognisant of the importance of accuracy of data. Errors with coding could lead to misrepresentation of data. It proved invaluable for the researcher to verify coding of data by conducting wild code checks to identify possible errors.

After the coding process the researcher obtained results of each variable measured, which was summarised in Chapter 5 as a representation of data from the research conducted.

3.9.3 Data Cleaning

The researcher acknowledges the importance of accurate data as errors would threaten the validity of measures and mislead the results of the data collected (Neuman, 2006). This could ruin the entire research project. Through random sampling the researcher checked for coding errors, with the use of wild code error checks.

3.10 Hypothesis

Hypothesis is a statement of prediction and a tentative answer to a research problem expressed in the relationship between dependant and independent variables (Frankfort-Nachmias & Nachmias, 1992). According to Trochim (2006) there is no formal hypothesis and the purpose of the study is to explore an area thoroughly in order to develop some specific hypothesis or prediction that can be tested in future research.

While studying the subject matter in detail, the following perceptions cropped up. The following hypotheses were formulated and will be tested during the subsequent stages of this research to confirm or dispute the perceptions.

3.10.1 **Testing correlation between annual budget and percentage budget spent on IS**

The null hypothesis (Ho) being:

"There is no correlation between the annual budget and the percentage budget spent on IS".

3.10.2 **Testing correlation between the implementation of standards for compliance and implementation of standards for certification**

The null hypothesis (Ho) being:

"There is no correlation between implementing standards for compliance and implementing standards for certification"

3.10.3 **Testing correlation between the presence of a security policy and application of security policies**

The null hypothesis (Ho) being:

"There is no correlation between the presence of a security of a policy and the application of a security policy."

3.10.4 **Testing correlation between an implemented information security awareness programme and staff regularly attends the programme**

The null hypothesis (Ho) being:

"There is no correlation between an implemented an information security awareness programme and staff regularly attends programme"

3.10.5 **Testing the correlation between clearly defined roles and responsibilities for the department and dedicated staff to manage IS.**

The null hypothesis (Ho) being:

"There is no correlation between clearly defined roles and responsibilities for the department and dedicated staff to manage IS."

3.11 Nonparametric tests

According Dallal (2000) data obtained from the questionnaire approach can be best analysed and tested using nonparametric test, which are also referred to as distribution-free tests. Nonparametric test do not require the assumption of normality or the assumption of homogeneity of variance. The tests are used to compare medians rather than means, and a favoured for the following reasons:

(i) This tests are more suitable for analysing ranked, scaled and rated data as set in the questionnaire;

(ii) These tests involve relative fewer arithmetic computations as compared to parametric tests and are most likely to be applicable for surveys as this is being undertaken;

(iii) These tests require no more or less restricting assumptions than the corresponding tests; and

(iv) These tests can be used to provide reasonably good results even for small samples.

Bivariate Relationships

These relationships allow the researcher to describe the relations between 2 variables, namely X and Y (Neuman, 2006). It allows the researcher to compare things that need to go together. As in the instance with the survey questionnaire there were a multitude of questions that needed to go together, which will reveal critical information to the researcher. These relationships that will be discussed in more detail are:

i) The departments' annual IT budget vs percentage IT budget spent on IS;

ii) Documented security policy vs the roles and responsibilities for IS in our department is clearly defined;

iii) Department have implemented security standards ISO17799:2000 vs we have implemented for compliance or certification;

iv) Department has implemented an IS awareness programme vs our staff receives regular IS awareness training;

Correlation (r) is the degree to which two variables are consistently related to each other. It could be positive or negative. Should the correlation be negative the two variables are unrelated to each other (Neuman, 2006). The closer the correlation to -1 and +1, the stronger the relation than the closer the relation to 0 the weaker the correlation.

3.12 Validity and Reliability

Validity refers to the credibility and correct use of a measuring instrument to attain specific results (Maxwell, 1996).

External validity can be defined as the ability to generalise for a research to a larger population (Kalof et al., 2007). The questionnaire compiled was derived from validated questionnaires (Ernst & Young, 2004), thus validity would be fairly high. In addition stratified sampling was used to obtain a representative sample from the population. In this instance the researcher used a survey questionnaire as a measuring instrument, which was standardised for the entire sample.

According to Shuttleworth (2008) validity and reliability are the cornerstones for scientific research, be it quantitative or qualitative, thus eliminating doubt. Reliability is when other researchers are able to perform the same research

and generate the same results, which will reinforce findings and acceptance of hypothesis. To ensure reliability, the questionnaire was provided to a pilot group, of which the responses varied very little which proved the questionnaire was reliable.

3.13 Limitations

No research conducted is immune to limitations. The researcher has identified potential limitations as listed below:

- The researcher was unable to utilise a survey questionnaire that is online, as the recommended online method, namely Survey Monkey, has limitations with the total number of questions it accepted for distribution.
- Surveying senior managers of the public service would prove difficult to reach and the survey might be intercepted by personal assistants (Neuman, 2006). The researcher was fortunate that she was afforded the opportunity to distribute the survey at an annual function where representatives across national and provincial departments would be in attendance. The researcher sought permission from the host, who agreed to honour the request. A covering letter, consisting of an introduction and outlining the objective of the research was drafted and attached to the distributed questionnaire. The researcher made her contact details available should the respondent wish to verify this information.
- The researcher is currently in the employ of government's IT agency. This organisation is responsible for implementing government's information and communication technology requirements. This could lead to bias on the part of the researcher.

3.14 Conclusion

Credible research should be supported by appropriate methodologies for it to be effective. Statistical techniques are an integral part of research, but without the interpretation of such results would give a diluted view of the reality.

In this chapter the researcher defined the methodology, identified appropriate techniques and statistical tests were used to test hypotheses were put forward.

The chapter to follow is critical as the actual data that was gathered, coded, analysed and interpreted would follow. This will inform or reject the

perceptions created, during the literature review. The findings would prove helpful to understand factors of non-compliance of information security management in the public sector of South Africa.

Chapter 4 – Presentation of Results

4. 1 Introduction

Chapter 3 formed the foundation for the methodology of the research work to be conducted in the field, hypotheses tested, findings analysed and reported.

The purpose of this chapter is to present the findings of the survey in an analytical form so that the hypotheses can be tested and clear conclusions can be drawn, firstly through an overview of the response analysis, followed by a series of statistical runs to test the results in line with the hypotheses set.

The data collected was analysed, using descriptive and inferential statistics.
The data collected through the survey questionnaire were coded and captured into spreadsheets for ease of clarification. It was then computed and analysed using statistical tools and software. MS EXCEL and Analyse-It (Microsoft Corp., 2010) and Analyse-IT (Analyse IT, 2010) were among the tools used to analyse the data. These tools were best suited in terms of diversity of tests and use of use of the software, to perform a variety of statistical test, such as Correlation and to determine probability (p), to establish whether the hypotheses should be accepted or rejected.

4.2 Overview of Analysis

MS EXCEL was used to generate Table 4-1. Out of the 100 Senior Managers surveyed and acceptable sample size of 100 was computed using Raosoft online tool (Raosoft, 2010). The calculation of sample size was based on the following parameters:

- 95% confidence level
- 5% acceptable margin of error
- 100% response distribution

While the confidence level indicates the amount of uncertainty that can be tolerated, the margin of error defines the amount of error that can be accepted in the present research. The percentages used for confidence level and margin of error may vary from research to research. A confidence level of

95% and 5% margin of error have laid foundation for drawing acceptable conclusions on the population (Murphy, 2004).

A response rate of 100% and refusal rate of 0% were obtained as depicted in Table 4-1 below:

Description	Number	%
Population	100	-
Acceptable Sample Size		-
No. of Responses (Obtained)	100	100%
Number of Refused responses	0	0%

Table 4-1: Response Overview

The overall response rate is acceptable as it higher than 65% (Saferpak, 2005). The overall response rate of 100% provides a comfortable foundation for statistical analysis and interpretation (NCES, 2005).

4.2.1 Analysis of Respondents profile

MS EXCEL was used to compile and graphically present the results gathered on respondents' positions within public service. From the responses obtained, 18% were HOD's, 8% CIO's, 42% IT Managers, 5% IT Security Managers, 0% IT Security Managers, 11% IT Specialist and 16% Lines of Business Managers, as presented in Table 4-2 Profile of Respondents.

Departmental Position	HOD	CIO	IT Mng	IT Sec Mng	IT Sec Consultant	IT Spec	LOB Mng
Number of respondents	18	8	42	5	0	11	16

Table 4-2: Profile of Respondents

Figure 1 given below, were Senior Managers in public service surveyed, held positions, ranging from HOD's, CIO's, IT Managers, IT Security Managers, IT Specialist and Lines of Business Managers. The main objective of this survey was to obtain input from this target group to ensure a realistic picture from Senior Management could be drawn. One has to note that there was no respondent fulfilling the role of IT Security Consultant and that only 5% of

respondents fulfilled the role of IT Security Manager. This rate could be deemed very low, as organisations are not giving sufficient attention to IT Security positions within their organisational structures.

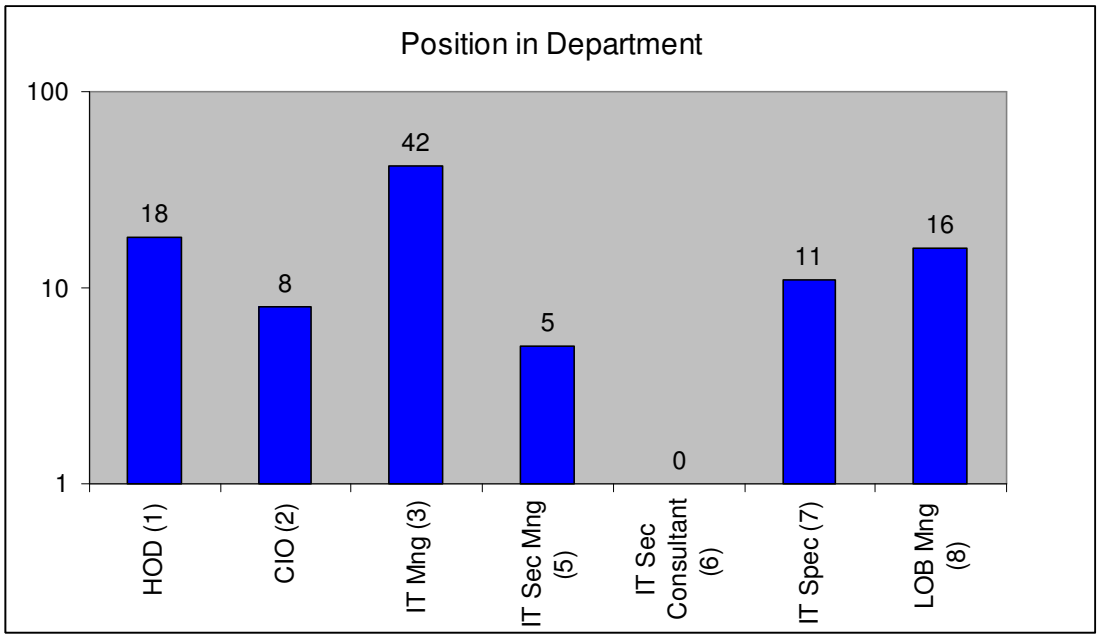

Figure 1: Position in Department

Analysis of Total number of employees employed in the department

MS EXCEL was used to compile and graphically present the results gathered of the total number of employees employed in the department. From the survey sampled of 100 respondents, 62% indicated they have 499 and less employees, 17% has less than 999 and 400, 10% has less than 1999 and 1000, 3% has less than 2999 and 2000, 2% has 3999 and 3000, 0% has 4999 and greater than 4000; and 6% has more than 5000 employees employed in the department, as presented in Figure 2: Analysis of total number of employees employed in department.

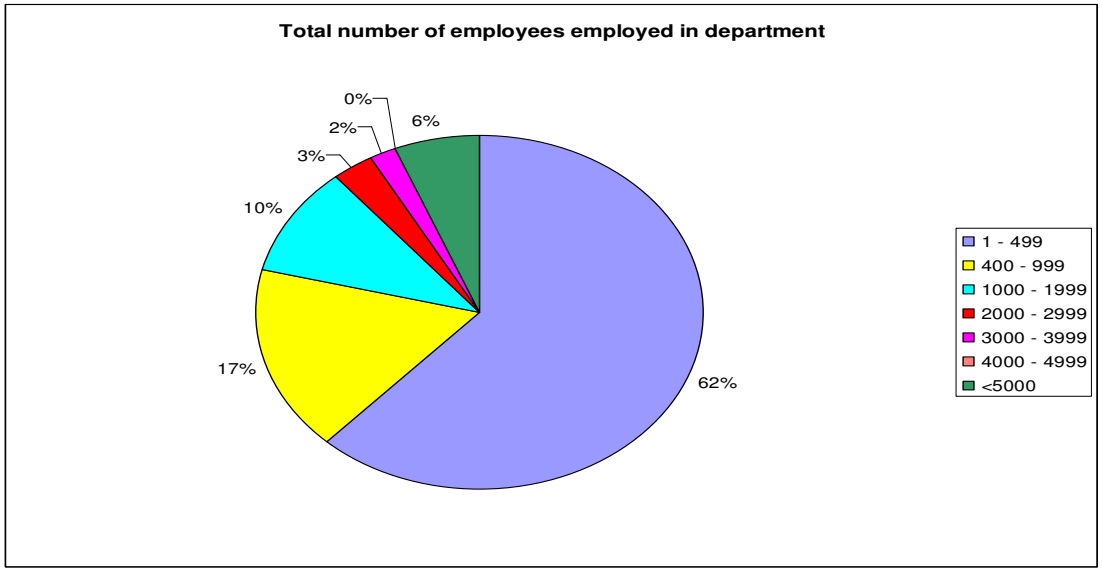

Figure 2: Analysis of total number of employees employed in department

4.2.3 Analysis of Annual IT Budget

The analysis of Annual IT Budgets was done using MS EXCEL to compile and graphically present the results gathered from departments. Information obtained related IT Budgets, 34% of respondents indicated their annual IT budget is between R1m to R5m, 19% between R5.1m – R10m, 14% between R10.1m – R50, 12% between R50.1m – R100m and 21% between R100.1m – more as shown in figure 3 Analysis of Annual IT Budget.

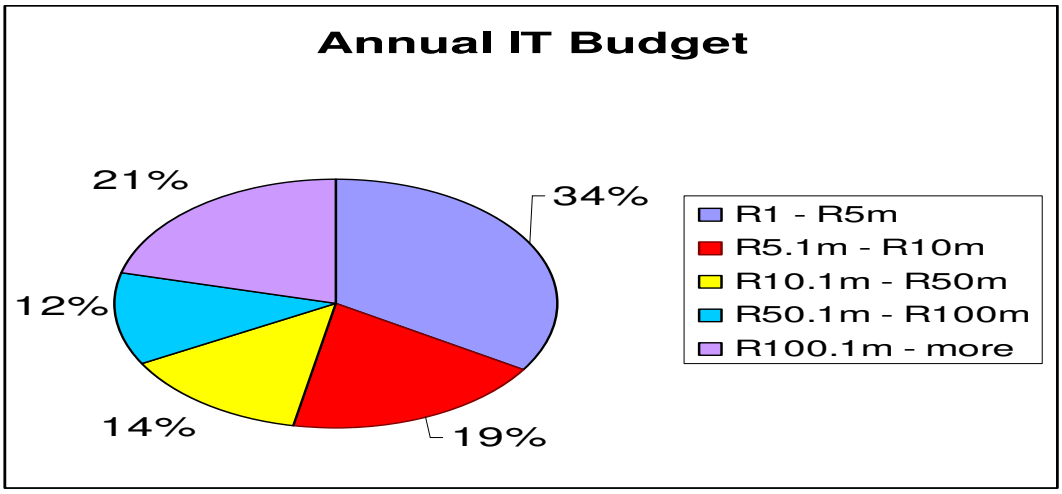

Figure 3: Analysis of Annual IT Budget

MS EXCEL was used to compile and graphically present the results gathered of the total Annual IS Budget from departments. From the surveyed sample of 100, 72% of the respondents indicated the department spent less than 10% of this budget on IS annually, 22% spent between 20% to 30%, 4% spent between 31% to 40%, whilst 2% of the respondents indicated they spend more than 50% of their IT budget on IS.

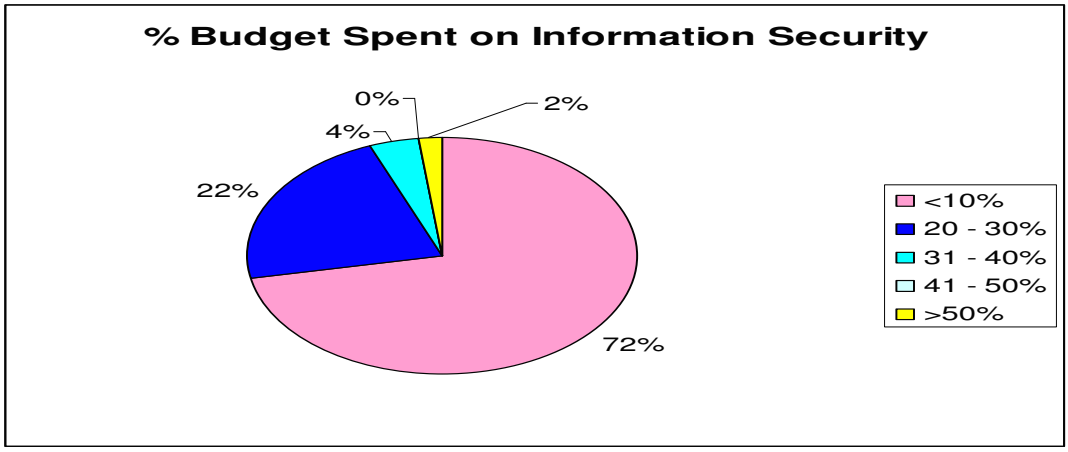

Figure 4: Analysis of Percentage Budget Spent on IS

The budgetary spent on IS was enlightening, as overall departments spent a significantly low amount (10%) of their annual budgets on IS, which is critical to secure information.

4.2.4 Analysis on Dependency on IT

MS EXCEL was used to compile and graphically present the results gathered of the departments dependency on IT, the 100 respondents surveyed, 82% of the respondents strongly agreed that their departments have a dependency on IT, whilst 16% agreed their department's dependency and only 2% of the respondents had a neutral position on the matter as shown in Figure 5: Analysis on Departments dependency on IT.

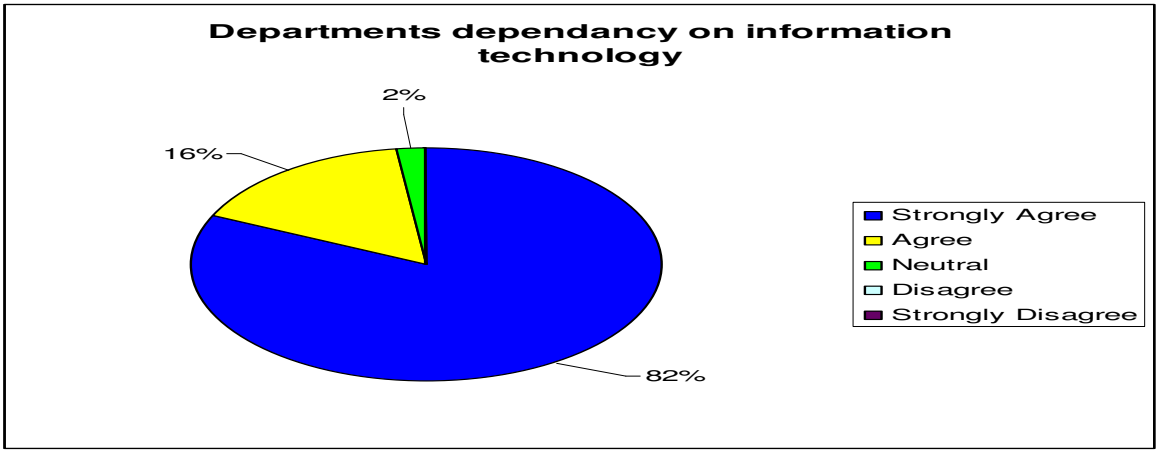

Figure 5: Analysis on Departments dependency on IT

4.2.5 Analysis on Total number users with internet access

MS EXCEL was used to compile and graphically present the results gathered of show the total number of users with internet access. 41% Indicated that <99 employees has access to the internet, 18% which represents a total of 100 to 499 employees, 13% which represents between >500 and <999, 20% which represents >1000 and <9999; 8% which represents >10 000 and < 49 999 employees has internet access, as shown in Figure 6 Analysis on Total number of users with internet access.

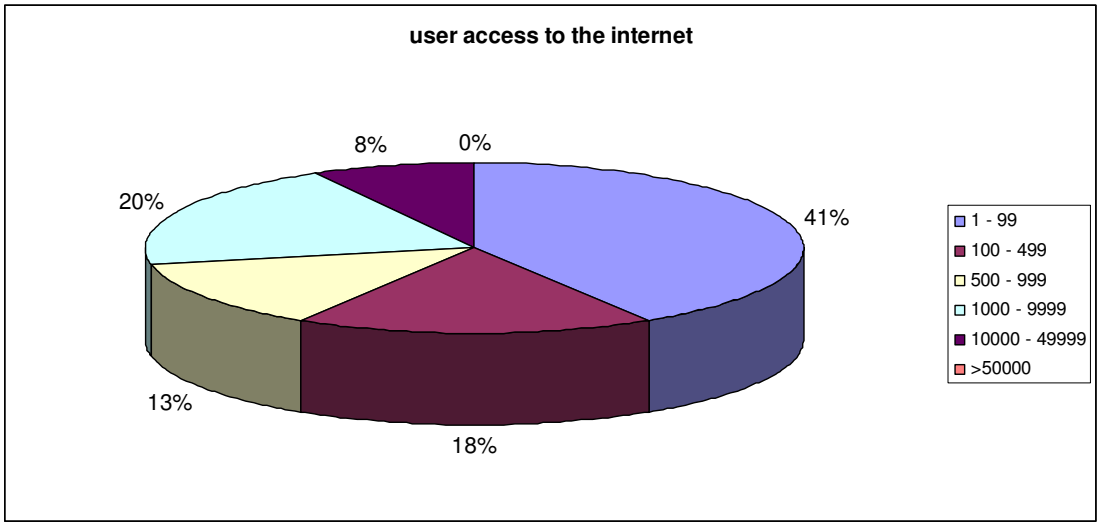

Figure 6: Analysis on Total number of users with access to Internet

4.2.6 Analysis on Computers used to store sensitive information

MS EXCEL was used to compile and graphically present the results gathered to determine whether computers were used to store sensitive information, from the 100 respondents surveyed, they indicated 43% store Strategic and or business plans, 28% store personnel records, 17% store own confidential information, 7% store blue prints, formulas and inventions; 4% store customer records and 1% store citizen or customer confidential information on personal computers, as shown in Figure 7: Analysis on computers used to handle/store sensitive information below:

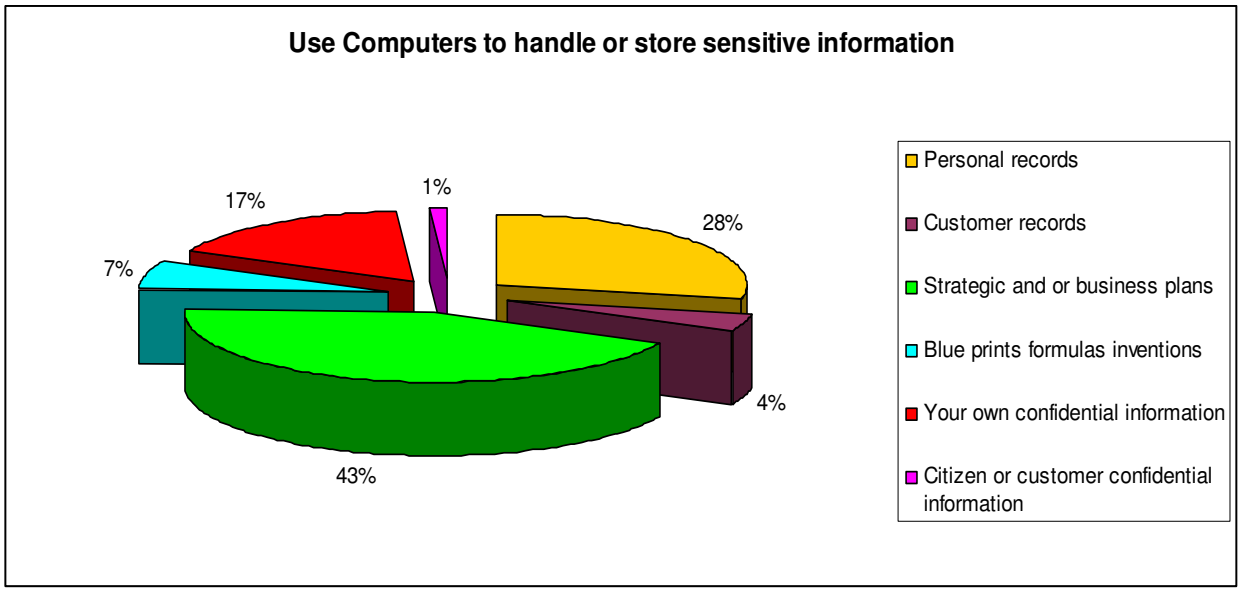

Figure 7: Analysis on computers used to handle/store sensitive information

4.2.7 Analysis concern with information leaking

MS EXCEL was used to compile and graphically present the results gathered to determine concerns with information leaking, from the 100 respondents surveyed, 86% indicated they are concerned with information leaking from their respective departments, whilst 14% indicated they are not concerned, as shown in Figure 8: Analysis on concern with information leaking, below:

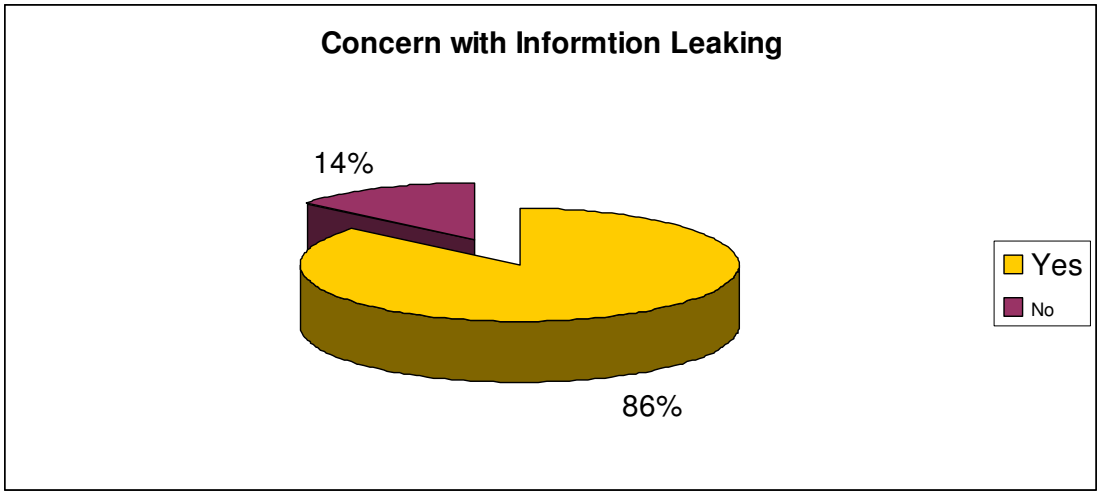

Figure 8: Analysis on concern with Information Leaking

4.2.8 Analysis of confidentiality compromised, who is most at risk

MS EXCEL was used to compile and graphically present the results gathered to determine analysis of confidentiality compromised, who is most at risk, 59% of the respondents indicated the department would be most at risk, 26% of the respondents indicated the employee would be most at risk, whilst 15% indicated the citizen would be most at risk, as shown in Figure 9 below:

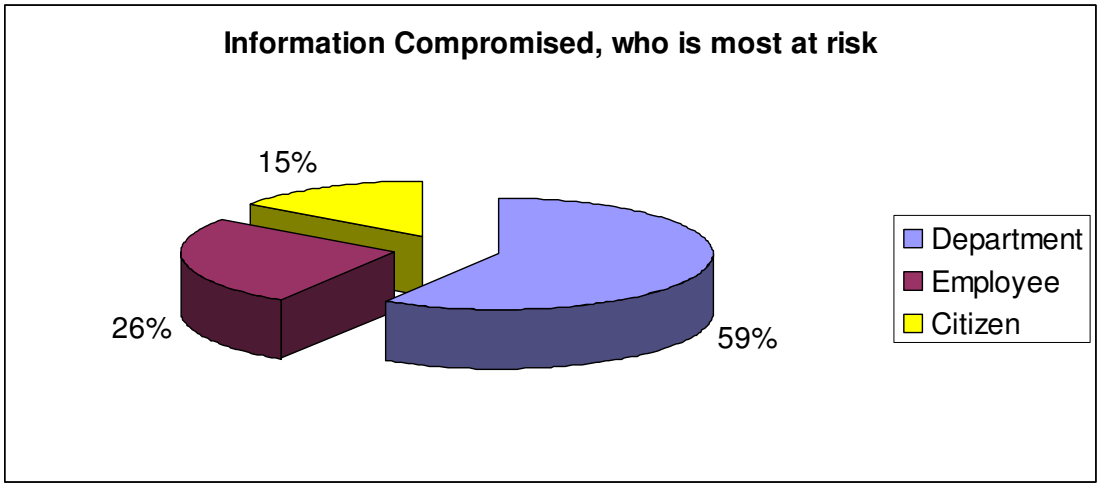

Figure 9: Analysis on Information Compromised, who is most at risk

4.2.9 Analysis of Information Security is important to our department

MS EXCEL was used to compile and graphically present the results gathered to determine if information security is important to the department, the respondents of 100 sampled 57% Strongly Agreed and 31% Agreed that information security is important to their departments. 8% remained neutral, whilst 2% Disagreed and Strongly Disagreed respectively.

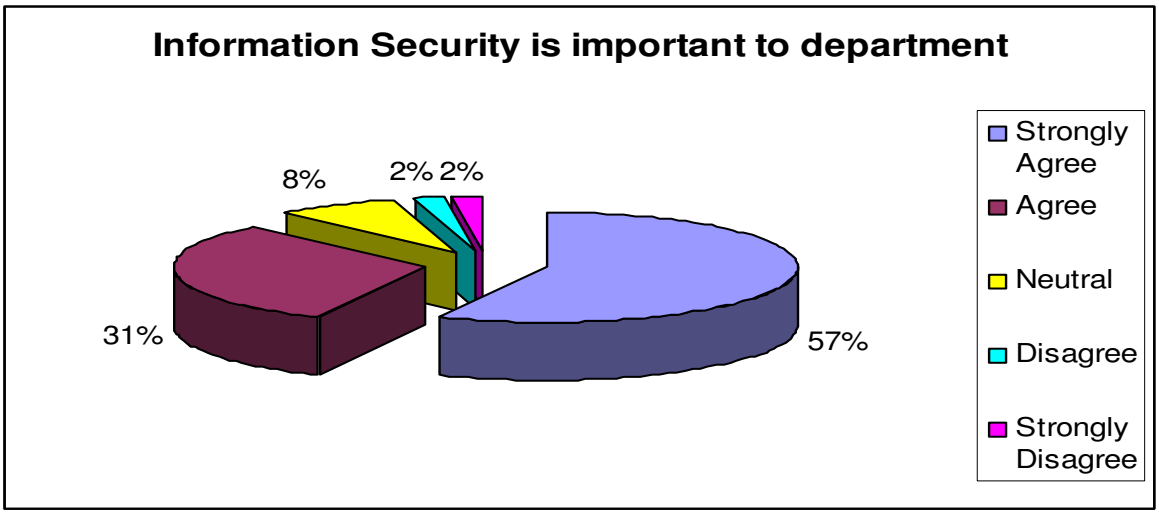

Figure 10: Analysis of Information Security is important to department

4.3 Section B - Governance

In this section the researcher focussed on key areas such as governance, IS standards, namely the British Standards and ISO Standards and components contained within the MISS to determine if departments do comply with relevant legislation. Through analysis of the data collected the researcher determined the following:

4.3.1 Analysis of dedicated staff to manage IS

MS EXCEL was used to compile and graphically present the results gathered on dedicated staff to manage IS, from the 100 respondents surveyed, 34% strongly agreed and 46% agreed that they have dedicated staff to manage IS, whilst 12% disagreed and 2% strongly disagreed that they have dedicate staff to manage IS.

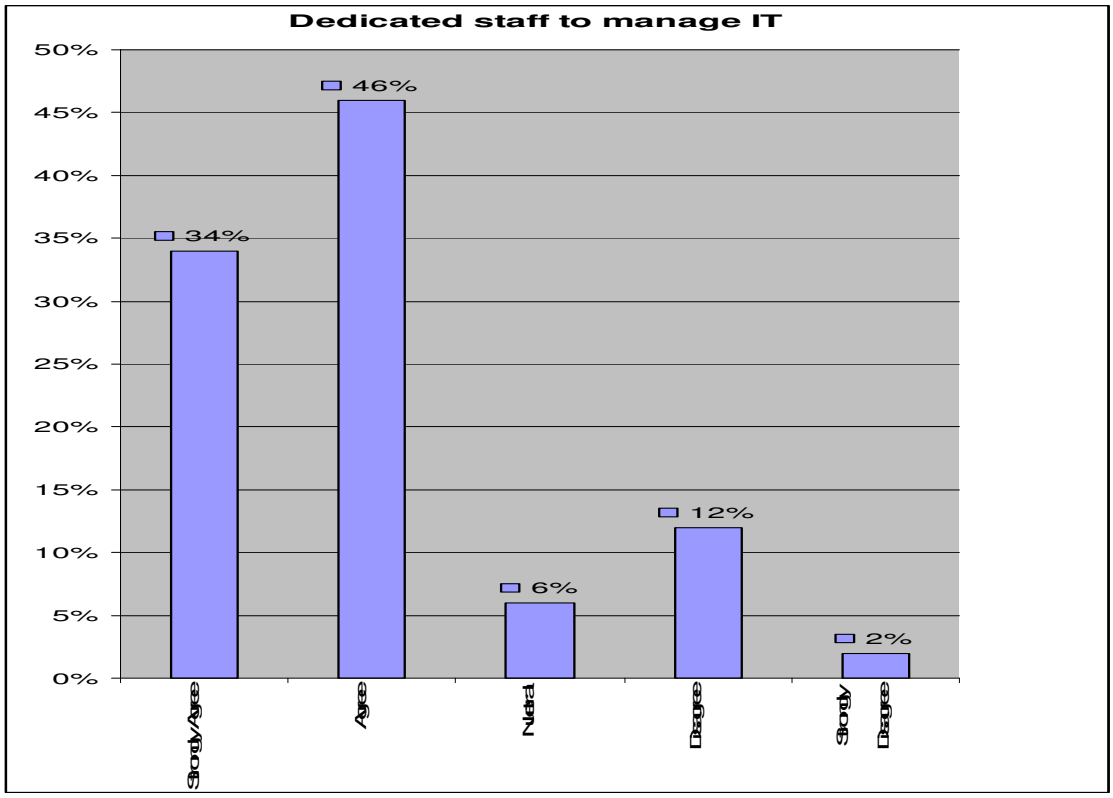

Figure 7: Analysis of dedicated staff to manage IS

4.3.2 Analysis of roles and responsibilities for IS is well defined

MS EXCEL was used to compile and graphically present the results gathered to determine an analysis of the roles and responsibilities for IS, is well defined 28% strongly agreed and 46% of the respondents agreed that the roles and responsibilities for IS in the department is well defined, whilst 17% disagreed.

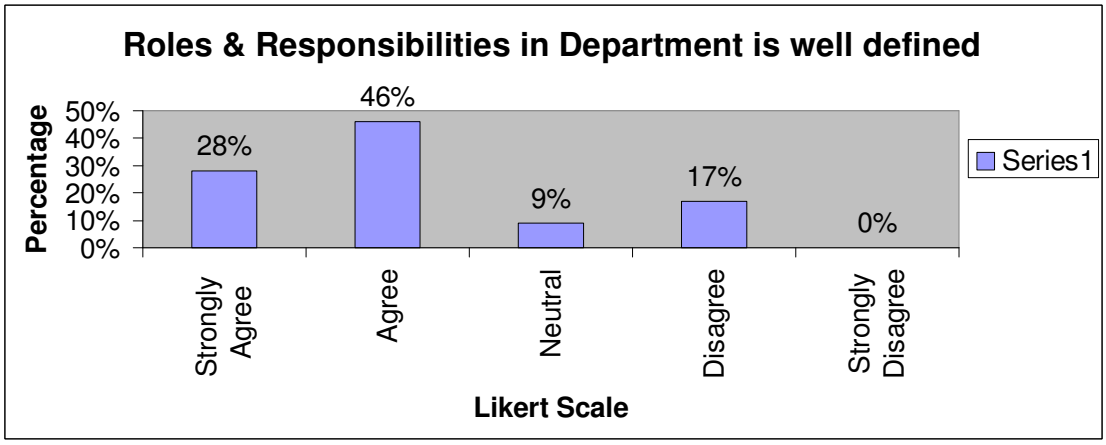

Figure 8: Analysis of roles and Responsibilities in department is well defined

4.3.3 Analysis of documented IT Policy

MS EXCEL was used to compile and graphically present the results gathered on the analysis of documented IT Policy, from the 100 respondents, 77% of the respondents indicated that they do have a documented IT Policy, whilst 23% indicated they do not have a document policy.

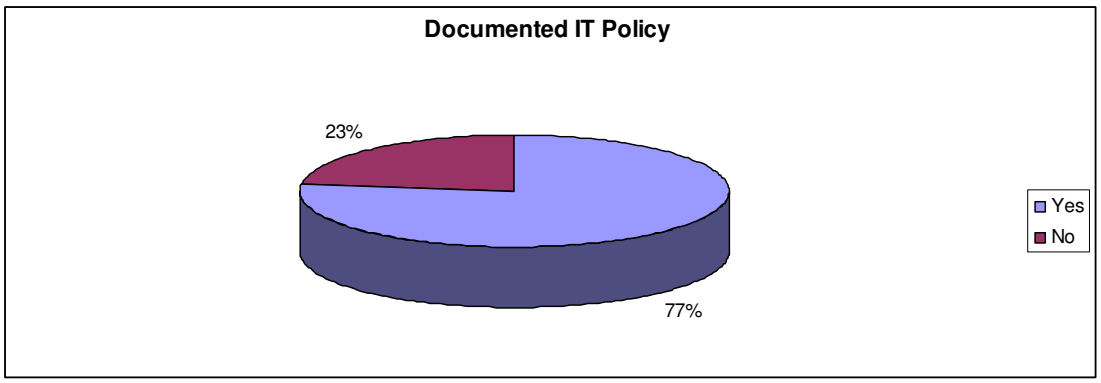

Figure 9: Analysis of documented IT Policy

4.3.4 Analysis of access to Information Assets

MS EXCEL was used to compile and graphically present the results gathered on the analysis of access to information assets, of the 100 respondents surveyed, 40% strongly agreed and 48% agreed that the department have appropriate physical and environmental security structures to safeguard areas that have ICT infrastructure that stores critical information, however 8% is neutral and 4% disagreed.

30% of the respondents strongly agree and 54% agree that the department can identify and locate all assets, including software, hardware, staff and services used for information handling, whilst 16% remained neutral and 6% disagreed.

24% of the respondents strongly agree and 54% agree that local access to information assets is adequately controlled, whilst 16% remain neutral and 6% disagreed that local access to information assets is not adequately controlled.

31% of the respondents strongly agreed and 53% agreed that remote access to information assets is adequately controlled, whilst 10% remains neutral and 6% disagreed that remote access is not adequately controlled.

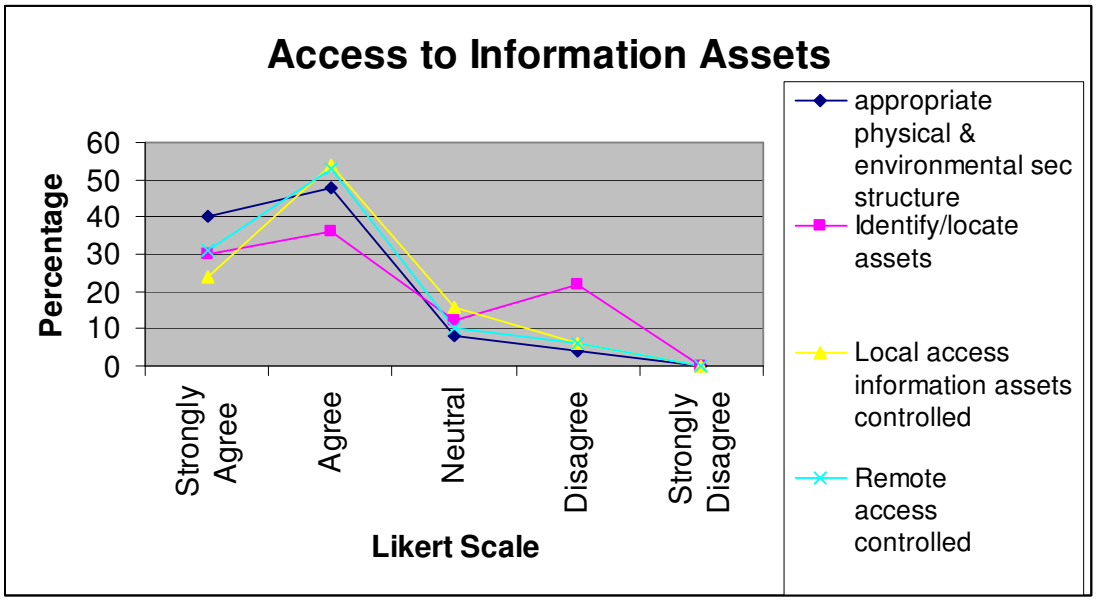

Figure 10: Analysis on access to Information Assets

4.3.5 Analysis of Business Continuity

MS EXCEL was used to compile and graphically present the results gathered on the analysis of business continuity, of the 100 respondents surveyed, 20% of the respondents strongly agreed and 32% agreed that their departments have business continuity plans in place that addresses the protection of critical business information to ensure continuity in the event of a disaster. However 22% of the respondents remains neutral, 16% disagreed and 10% strongly disagreed, indicating that their departments do not have business continuity plans in place that ensure a continuation of business in the event of a disaster.

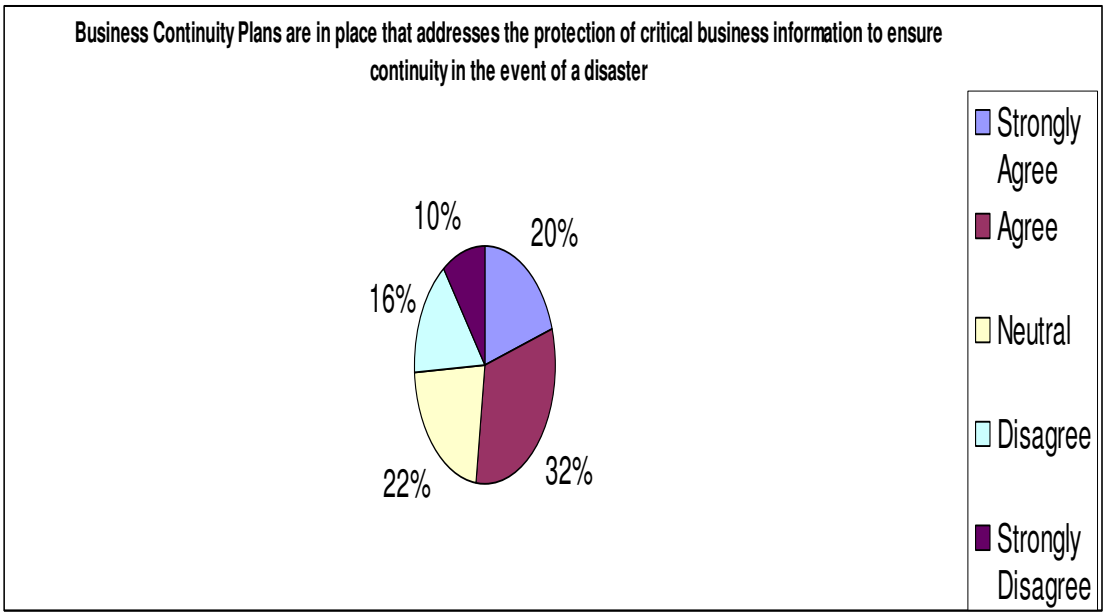

Figure 11: Analysis of Business Continuity

4.3.6 Analysis of the awareness IS Standards

MS EXCEL was used to compile and graphically present the results gathered on analysis of the IS Standard, of the 100 respondents surveyed, 71% of the respondents indicated that they are aware of the BS and ISO Standards, whilst 29% indicated they are not aware of these standards.

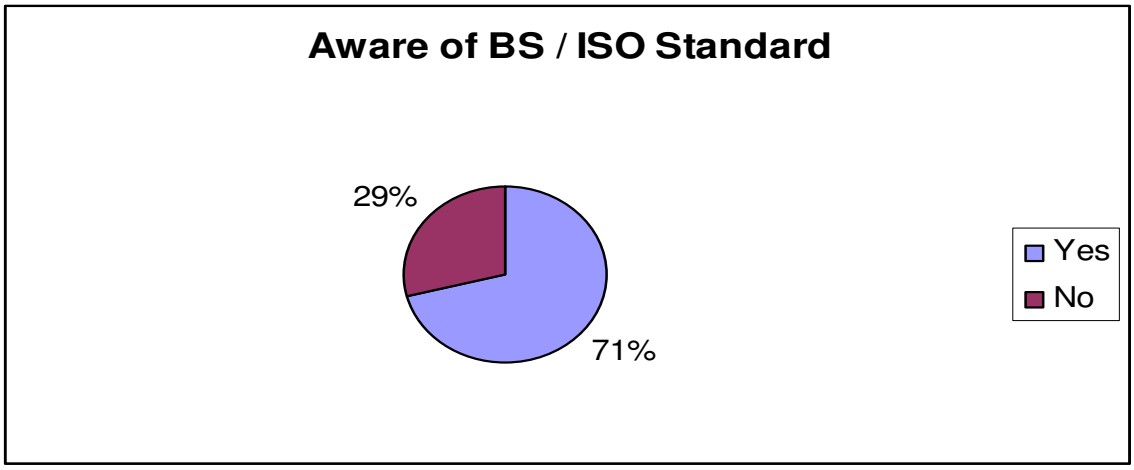

Figure 12: Analysis of the awareness of BS/ISO Standards

4.3.7 Analysis on the implementation of BS and ISO Standards

MS EXCEL was used to compile and graphically present the results gathered on the analysis of implemented BS and ISO Standards, of the 100 respondents surveyed, 20% strongly agreed and 22% agreed that their departments have implemented the BS and ISO Standards, whilst 22% remains neutral, 31% disagreed and 5% strongly disagreed that their departments have not implemented these standards.

12% strongly agreed and 40% agreed that their department has implemented the BS and ISO Standards for compliance, whilst 18% remains neutral, 25% disagreed and 5% strongly disagreed.

12% of the respondents strongly agreed and 24% agreed that their department has implemented the BS and ISO Standards for certification, whilst 30% remains neutral, 29% disagreed and 5% strongly disagreed.

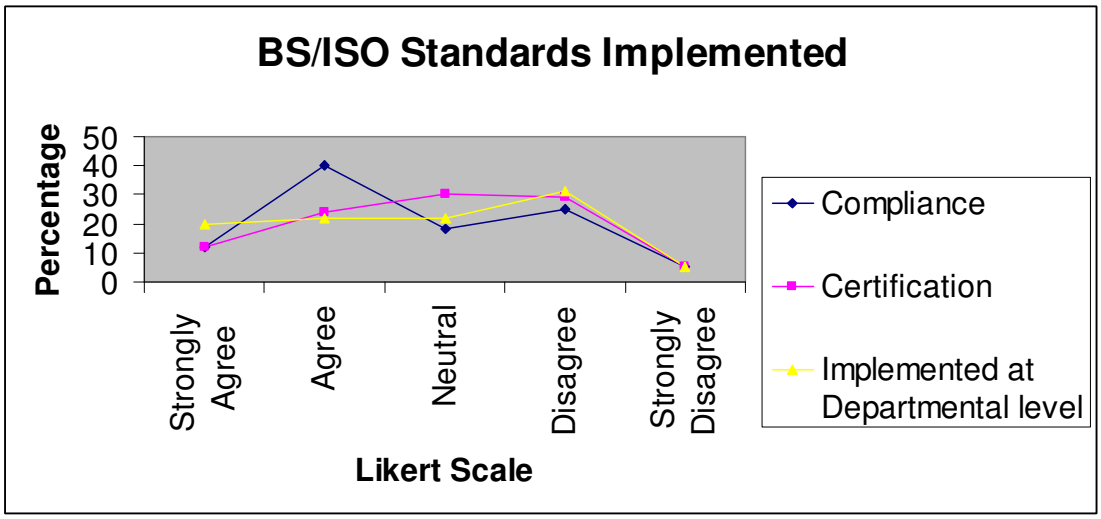

Figure 13: Analysis of BS/ISO Standards Implemented

4.4 Section C - IS Awareness

4.4.1 Analysis on IS regarded as high priority

MS EXCEL was used to compile and graphically present the results gathered on the analysis of IS regarded as high priority, of the 100 respondents surveyed, 50% strongly agreed and 38% agreed that their department regards IS as high priority, whilst 2% remained neutral, 8% disagreed and 2% strongly disagreed that IS is not high on the agenda of their department.

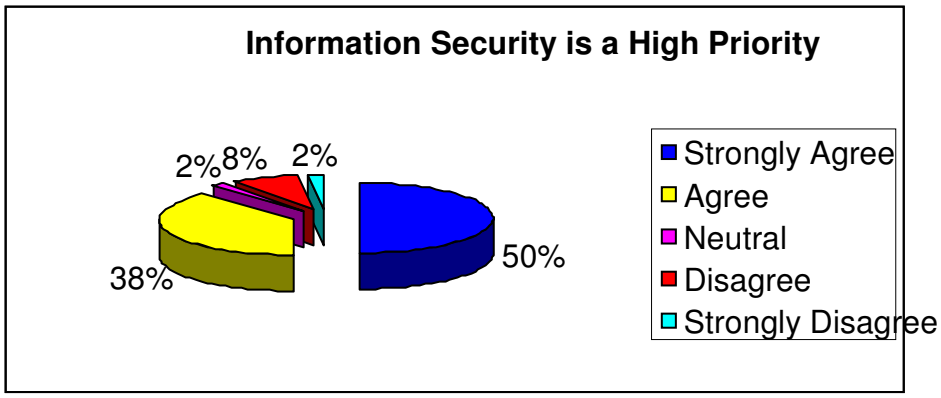

Figure 14: Analysis on IS as a High Priority

4.4.2 Analysis on IS Awareness Training

MS EXCEL was used to compile and graphically present the results gathered on the analysis of IS awareness training, of the 100 respondents surveyed, 28% indicated that staff members received IS awareness training annually, 38% indicated that staff received IS awareness training quarterly and 20% of respondents indicated that staff only received IS awareness training at induction when newly appointed in the department.

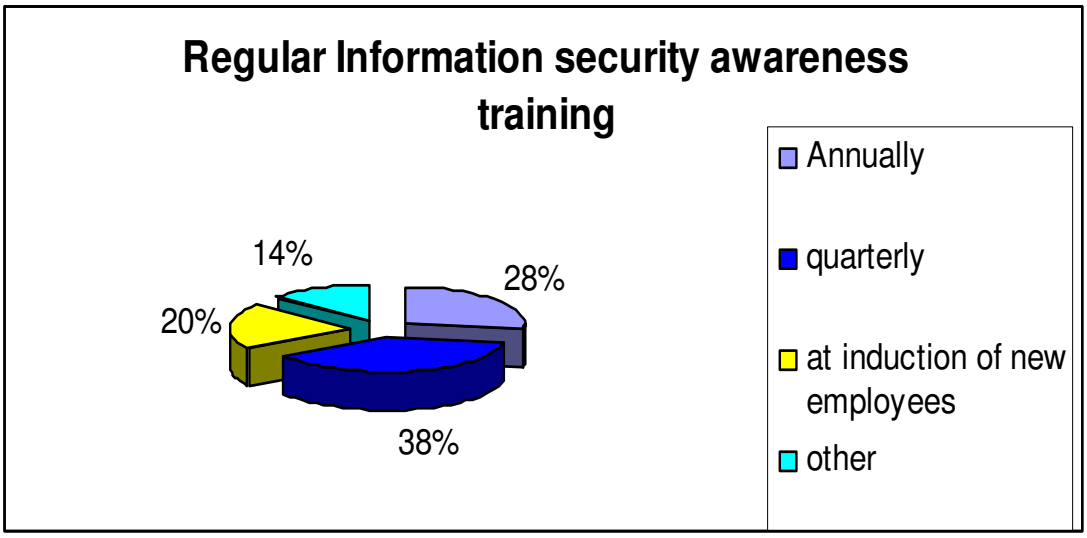

Figure 15: Analysis on regular IS Awareness Training

4.4.3 Analysis on compulsory Security Awareness Programme

MS EXCEL was used to compile and graphically present the results gathered on the analysis on compulsory security awareness programmes, of the 100 respondents surveyed 62% indicated that the departmental IS awareness programme is compulsory whilst 38% of respondents indicated IS awareness programmes within the department is not compulsory.

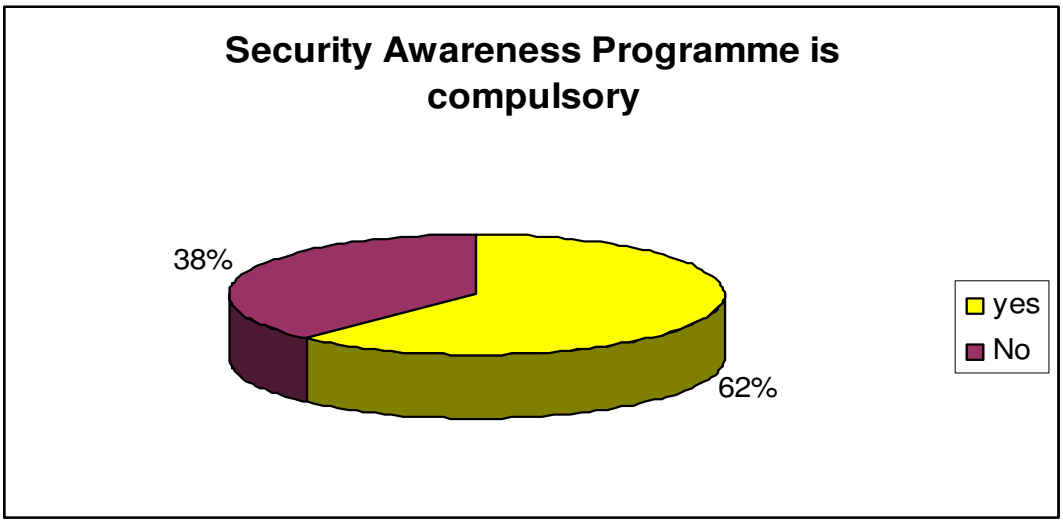

Figure 16: Analysis on Security Awareness Programme is compulsory

4.4.4. Analysis on periodically reviewed IS Awareness Programme

MS EXCEL was used to compile and graphically present the results gathered on analysis of periodically reviewed IS awareness programme, of the 100 respondents surveyed 14% strongly agreed and 45% agreed that departmental IS awareness programmes are reviewed periodically, 20% remained neutral,19% disagreed and 2% strongly disagreed that IS awareness programmes are not reviewed periodically.

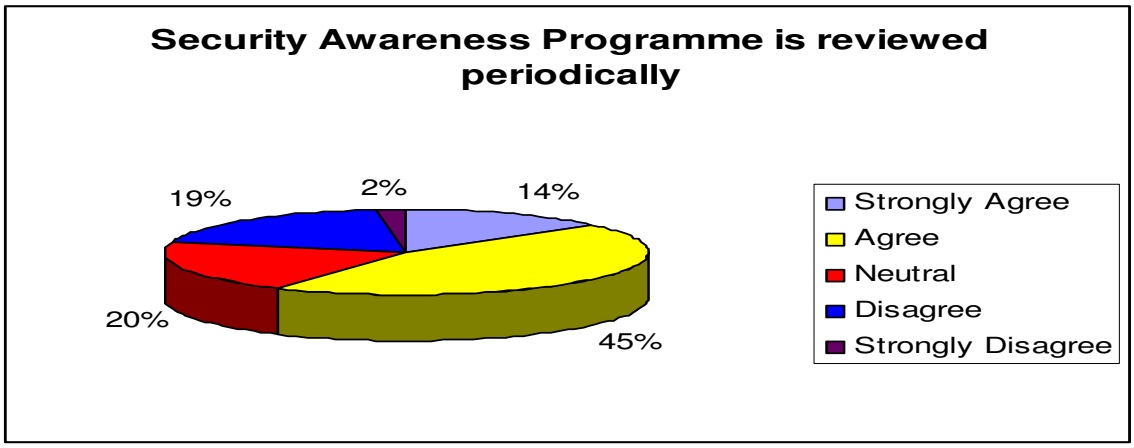

Figure 17: IS Awareness Programme is reviewed periodically

4.4.5 Analysis of Regular updates on IS threats

MS EXCEL was used to compile and graphically present the results gathered on the analysis of regular updates on IS threats, of the 100 respondents surveyed, 18% strongly agreed and 27% agreed that staff receive regular updates on IS threats. 28% remained neutral on the matter whilst 21% disagreed and 6% strongly disagreed that indicating that staff do not receive regular updates on IS threats.

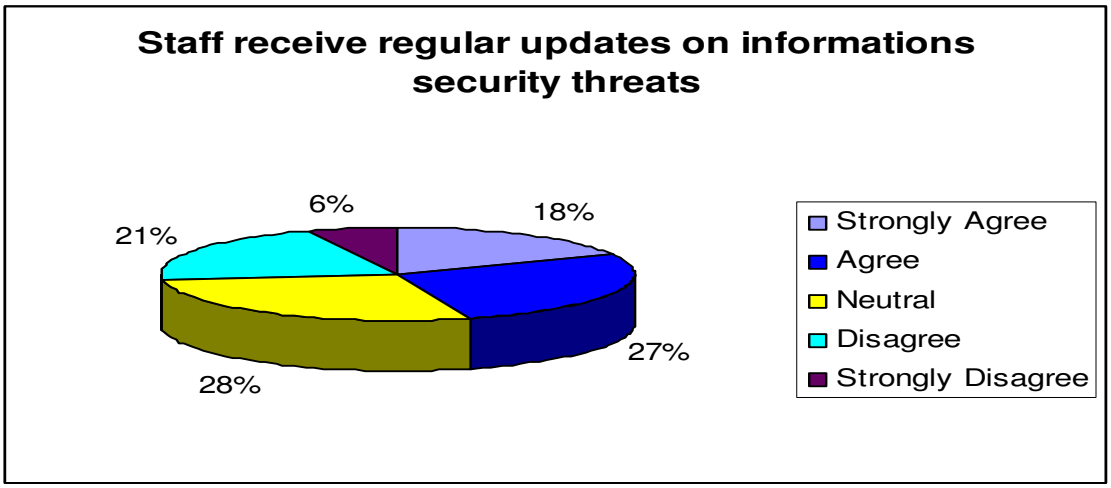

Figure 18: Staff receives regular updates on IS threats

4.4.6 Analysis of Security topics

MS EXCEL was used to compile and graphically present the results gathered on analysis of awareness of security topics, of the 100 respondents surveyed, they responded that staff is aware of the security topics as follow:

e-mail & electronic communication	physical security / access to buildings	passwords	internet security	Responsibilities of information security	Viruses	software licensing & copyright
71	73	78	21	21	45	21

security incident reporting	security updates and patches	mobile phones & PDA's	security out of office	personal use of corporate equipment	phishing	clear desk policy	instant messaging
20	25	21	15	20	29	34	11

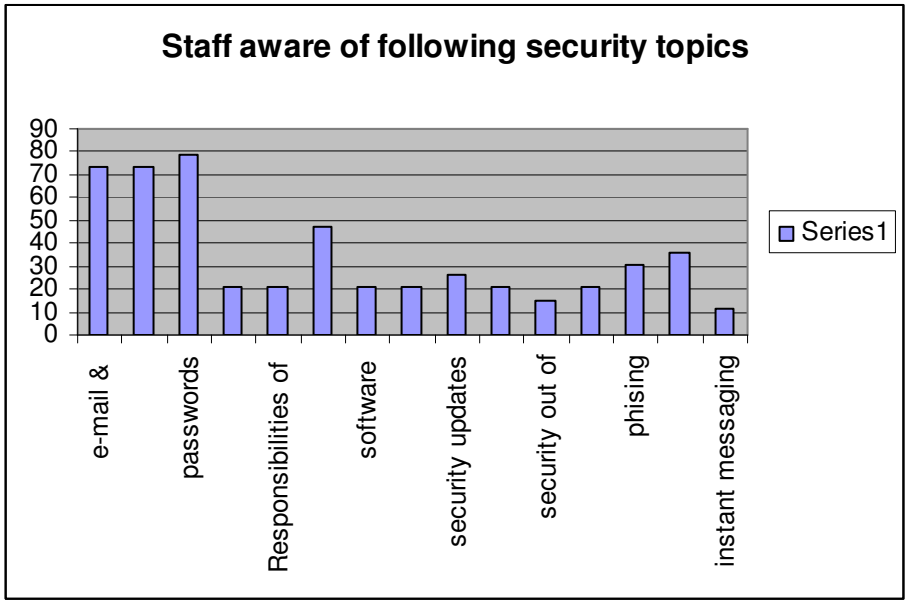

Figure 19: Analysis on awareness of IS Topics

4.4.7 Analysis on techniques effective of raising IS

MS EXCEL was used to compile and graphically present the results gathered on the analysis of effective techniques for raising awareness on IS, of the 100 respondents surveyed, they responded as follow:

Technique	**Response**
Induction	70%
Security Policy	67%
Letter of Appointment	58%
Classroom training	37%
Computer based training	22%
Intranet site	16%
Poster campaigns, regular newsletters and promotional material	13%

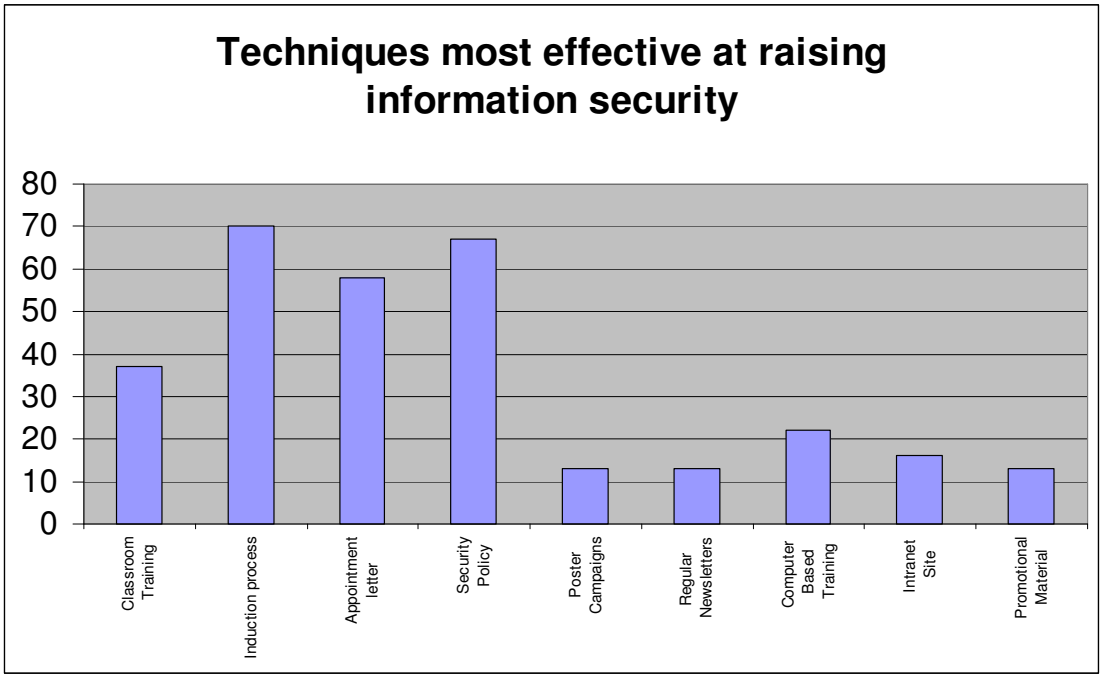

Figure 20: Analysis on effective techniques at raising IS awareness

4.5 Conclusion

The aim of this chapter was to highlight the key findings of the research work undertaken to investigate factors of non-compliance of information security management in the public sector of South Africa.

Data was compiled, coded and tabulated in such a way that it could be used for analysis and interpretation. The techniques utilised, assisted with interpretation of the sampled data and statistical tests were used with the support of specialized tools with the view of testing the hypotheses that were put forward, in order to clarify perceptions earlier formulated.

From the data analysed, one can note that Senior Managers in the public service do have an increased awareness of threats against information as the respondents surveyed, the researcher concluded that 82% of the respondents strongly agreed that their departments have a great dependency on IT and 86% of the respondents concurred that they are concerned with information leaking as the department, employees and citizens would be most at risk. Overall the respondents indicated that they spend less than 10% of their annual budgets on IS to ensure the protection of information as an asset.

Senior management strongly agreed (50%) that IS is high on the agenda of their department and staff members receive IS awareness training on a

regular basis, with 38% confirming quarterly. Although 62% of respondents confirmed that IS awareness programmes are compulsory to employees within their department, a significant 38% indicated that it is not compulsory. IS awareness programmes reviewed periodically, and this was confirmed by the respondents of whom 14% strongly agreed and 45% agreed. Overall the respondents, 18% strongly agreed and 27% agreed that staff receive regular updates on IS threats and staff is well aware of security topics ranging from e-mail and electronic communication, passwords, physical security, access to buildings, internet security, viruses, software licensing and copyright, clear desk policy, etc. In order of priority they have indicated that the following methods have proved most effective at raising IS levels; namely Induction (71%), Security Policy (67%) and letter of appointment (58%).

Based on the MISS each department should have documented IS policies and 77% of the respondents surveyed indicated they do have these policies in place. 46% of these senior managers indicated that they have dedicated staff to manage their IS and their roles and responsibilities are clearly defined. Access to information as an asset should be highly controlled and 40% strongly agreed, 48% agreed that their departments have appropriate physical and environmental security structures in place to safeguard areas that have ICT infrastructure and stores critical information. 54% indicated that they are able to locate all assets including software, hardware, staff and services used for information handling. Local and remote access to information assets is controlled. 32% of the departments do have business continuity plans in place in the event of a disaster ensuring a continuation of services should the latter occur.

Although the overall majority (71%) are aware of both BS and ISO standards, less than half of the populations surveyed indicated that their department has implemented these standards. The reason for implementation was either for certification or compliance.

The finding gave a clear indication that the level of compliance with the MISS has room for significant improvement.

In the next chapter the researcher aims to interpret and analyse the findings of the research.

Chapter 5 Interpretation and Analysis of Findings

5.1 Introduction

In the preceding Chapters 1 to 4, the researcher focussed on conducting a literature review, determining the research methodology and presenting the data post the analysis of statistical data. Chapter 3 formed the foundation for the methodology of the research work to be conducted in the field, hypotheses tested, findings analysed and reported. In this chapter the researcher will present an analysis of the findings.

The objective of this research was to investigate factors of non-compliance of information security management in the public sector of South Africa.

The researcher deemed it appropriate to investigate such factors, as the increased usage of information and communication technologies in the public service have exposed and made the institution vulnerable to potential intrusions. Global trends indicate that Senior Managers are not implementing information security policies and procedures, although trends in the governance arena highlights the elevation of ISG to board of director and executive management levels, to ensure compliance with organisational policies. The South African public service has implemented the MISS with the objective to provide procedures and measures to protect government information that will impact the vulnerability of the state, should it be compromised. Therefore this research was necessary to determine such factors of compliance and identify areas that could be recommended for consideration of improvements.

5.2 Conceptual Framework

In order to fulfil the objectives of the research, the researcher developed a conceptual framework, which is described a broad set of ideas and principles from ISM, which was used to structure the presentation of the research report (Reichel & Ramey, 1987). The conceptual framework is a tool that develops awareness and understanding of the relevant field of enquiry, in this case

ISM. According to Guba and Lincoln (1989) the conceptual framework is an agenda of negotiation.

As in the case of this research, investigating factors of non-compliance of ISM in the public sector of South Africa, the researcher was able to explore corporate governance, IT Governance, ISG, international information security standards; South African legislation and definitions applicable to ISM to determine the impact on factors of non-compliance. In the past information security was assigned to the IT Manager, however there has been paradox and it now widely acceptable that all in the employ of the public service, management and staff should contribute to compliance with information security policy. With the acceptance of the Codes of Good Practice, King III Report, Members of the Board of Directors, CEOs and Managers at a strategic level are held accountable for the implementation of IS and executing of oversight responsibility in respect of governance to ensure compliance. These shifts are attributed to global developments in corporate governance and organisational acceptance of IS accountability.

A study conducted by Dagada, Eloff and Venter (2009) found that most organisations and government departments are in conflict with the spirit of good governance and do not take IS seriously, informed the development of the framework, the research design and the means of investigating the realities of the current situation (Smyth, 2002).

Goetz & LeCompte (1984) stated that a conceptual framework, assist the researcher with a roadmap to ensure the research process remains on track.

The objective of the conceptual framework is to provide the researcher with a roadmap, the researcher should be aware of the limitations of this concept as highlighted by Mason & Waywood (1996). Whereas Miles & Huberman (1994) advises the researcher to remain open to new and unexpected occurrences when reviewing data in the investigation process.

5.3 Governance

The researcher reviewed literature related to aspects of corporate governance, whereby Wixley and Everingham (2005) highlighted that this relates to the manner in which companies are governed and techniques used to direct and manage organisational performance to ensure the organisational

strategic objectives are met. As in the case of public service, this is all about service delivery to the citizens of South Africa. As information is regarded as a critical asset, ISM is pertinent to ensure optimal services are rendered. However there are interrelated components, such as management who ensures that such enforcement and compliance with such policies are takes place.

As was highlighted in the literature reviewed on ITG, whereby Van Grembergen, De Haes, & Guldentops (2004) stated that IG aligns IT with an organisations strategy to ensure maximum value is derived. However the ITGI, Brown (2006) and Petersent (2004) articulates ITG as the distribution of IT decision making rights and responsibilities amongst organisational stakeholders and the procedure and mechanisms for making monitoring strategic decisions regarding IT possible. Although brings about a myriad of organisational benefits, there are associated risks which cannot go unnoticed. Such risks include loss of assets, data fraud and theft; and business disruption (Warren et al., 1998; Gelinas et al., 1999; Beasley et al., 2000; Hermanson et al., 2000; Hadden et al., 2003 and Abu-Musa, 2006).

IS should not be regarded as a technical matter (Dodds & Hague, 2004), but as a critical component of corporate governance, which is a management responsibility to ensure enforcement and compliance (Von Solms, 2005). This implies that all components of the organisation, from the board of directors, executive management to the lowest level employee has critical role to ensure compliance with appropriate policies and procedures to ensure the protection of the organisations information.

ISG is defined as an essential component of corporate governance, ensuring management's commitment in achieving superior information security, enforced through appropriate organisational structures, appropriate policies and procedures, processes, technologies and compliance mechanism, ultimately ensuring the integrity, confidentiality and availability or organisational assets (Von Solms, 2006).

ISG as a critical component of corporate governance will ensure organisational adherence to internal control mechanisms and compliance with external legislation, regulations and policies, it is therefore incumbent upon the board of directors and management of the organisation to ensure such

mechanisms and or instruments are implemented. Furthermore the advent of King III (2010), Code of Corporate Governance it would be crucial for the researcher to determine the impact of this instrument and highlight the relevance to the research, compliance with MISS by senior managers in the public service.

5.4 Standardization and best practice

According to Zuckermann (1997) there are two kinds of organisations that exist globally, those who have embraced internal standards and those with the intent too. Evidence have emerged that the adoption and compliance with international standards, is central to the development of countries competiveness. Globally there has been a realisation that information is the impetus of economies, which is dependent on the secure flow, both within and outside of governments, across businesses, there information security is of critical importance, ensuring such transactions or exchanges are conducted with the utmost integrity.

Standardization will ensure that a common criterion exists throughout the public service ensuring that security is in place. It has become globally accepted that standards are a means to enforce good security practices. The adoption and compliance to attain certification of an international best practice will assist with organisational competitiveness and the public service would make a statement of its ability to manage IS.

The public service is inherently dependant on the confidentiality, availability and integrity of information (ISO/IEC 17799: viii) to deliver a service to the citizens of SA. This information should be seen as an asset, with considerable value and has to be protected at all costs. IS protects these assets, from a range of threats to ensure continuity in services. This will be achieved through the implementation of a range of processes, policies, procedures and controls. The information systems and networks of the public service are faced with security threats from a wide range of sources, which include cyber crime, that is computer assisted fraud, espionage and sabotage. These sources of damage such as viruses, hacking, and phishing have become increasingly sophisticated as cybercrime have become economically viable.

Certification creates access to global markets, protection of patents and the environment, government acquisition reforms and improves quality (Howie, 1995). This is further confirmed by Solms (2001) where he states that an organisations increased dependency on technology, increases its vulnerability and costs with positive spin-offs as the creation of new opportunities.

Individuals who handle this information play an important role and their behaviour towards IS will determine the level of risk and exposure. Behaviour and perception toward IS can be improved through continued awareness and training (Caralli and Wilson, 2003).

Standardisation of IS policy controls and procedures are proposed, ensuring adherence to corporate governance and international security standards enhancing organisational resilience and improving its competency in protecting its information asset.

5.5 Factors impacting ISM

Security objectives and activities must be conducted based on business objectives and requirements, led by the business management (Von Solms, 1998). During the literature review the researcher looked at the following factors during ISM implementation: people, culture, attitude, security education and training, ownership and responsibility as highlighted by Nosworthy (2000).

Managerial factors include top management support and commitment, security education and training and regulations. Additional critical factors are awareness and financial resources (Chang & Ho, 2006; Kankanhlli et al. 2003). This was extensively discussed in the aspects covering corporate governance, ITG and ISG.

5.6 Research methodology used

Research methodology forms an integral part of any research undertaken (Leedy, 1993). The methodology used will assist in explaining the nature of the data and the methods employed to generate appropriate conclusions.

For the purposes of this research report, quantitative analysis was deemed the most appropriate methodology as the researchers investigated factors of non-compliance of ISM in the public sector of South Africa.

Quantitative researchers seek explanations and predictions that generalise to other persons and places (Leedy and Ormrod, 2005), with the intention to establish, confirm or validate relationships that contribute to theory.

The researcher utilised a survey questionnaire as the instrument to obtain information from respondents representing the sample (Leedy and Ormrod, 2005). The survey questionnaire measured IS awareness, compliance with governance and international standards using the Likert scale based on a rating of 1 to 5 (Likert et. al Neuman, 2006). The survey questionnaire was distributed amongst the sample identified, targeting HOD's, CIO's, ICT Managers and Lines of Business Managers employed in the public service, they are directly responsible for both compliance and social aspects of ISM.

Primary data was obtained through the use of the survey questionnaire and secondary data was obtained from books, journals, case studies and articles.

Data analysis was conducted through the manipulation of quantitative data that allowed the researcher to reveal matters of interest obtained within the data about the population surveyed (Neuman, 2006). During the translation of the raw data, the researcher coded the data which represented values of variables which measures the characteristics of the respondents, subjects and other cases suitable for computers. This was achieved through the utilisation of EXCEL spreadsheets for tabulation.

5.7 Data Analysis

The data collected was analysed, using descriptive and inferential statistics.

The data collected through the survey questionnaire were coded and captured into spreadsheets for ease of clarification. It was then computed and analysed using statistical tools and software. MS EXCEL and Analyse-It (Microsoft Corp., 2010) and Analyse-IT (Analyse IT, 2010) were among the tools used to analyse the data. These tools were best suited in terms of diversity of tests and use of use of the software, to perform a variety of statistical test, such as Correlation and to determine probability (p), to establish whether the hypotheses should be accepted or rejected.

5.7.1 Statistical Tests

Having analysed the responses obtained, it is now possible to conduct certain well-devised statistical tests to support the analysis and confirm certain interpretations or assumptions. Five hypotheses were enumerated in Chapter 3 and were meant to be tested in this chapter on the basis of the findings of the survey. The primary reason for conducting these tests was to confirm or refute certain perceptions on compliance with ISM in the public service.

These tests were conducted with the assistance of Analyse-IT, using the data compiled and computed in MS EXCEL spreadsheet (Analyse-IT 2010).

Hypothesis Testing

5.7.1.1 Testing correlation between annual budget and percentage budget spent on IS

The null hypothesis (Ho) being:

"There is no correlation between the annual budget and the percentage budget spent on IS".

Test	**Pearson's Correlation**
Alternative hypothesis	**Annual IT Budget (X) = % Budget spent on IS**
Performed by	**Tania Abrahams**
Numerator: Σ(xy)-N($\bar{x}$ $\bar{y}$) =	97
Denominator: $\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}$ =	184.553
Pearson's *r* = $r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}}$	0.525594
R-squared =	0.276249
t = $t = \frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$	6.116025
Degrees of freedom =	98
Probability level (two-tailed) =	1.97E-08
Probability level (one-tailed) =	9.83E-09

p-value	<.0001

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variable are related, for the purposes of establishing whether or not there exists a correlation between the annual IT budget and the percentage budget spent allocated for IS.

The two variables in the hypothesis and the correlation test to be conducted are:

i) Annual IT Budget (X)

ii) Percentage budget spent on IS (Y)

The data collected for these two variables are nonparametric and the Spearman's Correlation technique will be used to test the null hypothesis (Siegel & Castellan, 1988). The data have been coded and ranked on the basis of their respective frequencies. The responses obtained from the survey were tabulated in MS Excel using pivot tables. The frequencies for variable (X) and (Y) were then ranked as per Spearmen Rank Technique independently from highest to lowest.

There were 100 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by (r). The Spearman's rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a relationship between two variables (Siegel & Castellan, 1998). A 95% confident interval (CI) was again used.

The closer r is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

The r value of 0.5255, as obtained above, suggest a fairly strongly relationship between the two variables, that is Annual IT Budget (X) and Percentage budget spent on IS (Y) and the computed t-test derived at 6.116

It is important for the researcher to report on the p-value, which is the probability of obtaining a value of the test statistic as extreme or more extreme, than actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

According Armitage & Berry (1994), the p-value and the confidence interval (CI) are computed around the observed proportion. The confidence interval utilised was 95%.

The p-value is the determining factor to accept or reject the null hypothesis. The p-value of 0.05 is the threshold used to evaluate the null hypothesis (iSixSigma, 2005). Researchers will reject a hypothesis with a p-value less than 0.05, however according Dallas (2000), a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence against the null hypothesis. Should the p-value be close to zero, it signifies a false hypothesis (iSixSigma, 2005).

On the basis of the result of the p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used. It indicates that Senior Managers in the public service does ensure that sufficient budget is allocated for IS spent.

5.7.1.2 Testing correlation between the implementation of standards for compliance and implementation of standards for certification

The null hypothesis (Ho) being:

"There is no correlation between implementing standards for compliance and implementing standards for certification"

Test	**Pearson's Correlation**
Alternative hypothesis	**Implementing standards for compliance = implementing standards for certification**
Performed by	**Tania Abrahams**
Numerator: Σ(xy)-N($\bar{x}$ $\bar{y}$) =	694
Denominator: $\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}$ =	784.368768
Pearson's *r* = $r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}}$	0.884787906
R-squared =	0.782849639
t = $t = \frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$	18.79628138
Degrees of freedom =	98
Probability level (two-tailed) =	2.87376E-34
Probability level (one-tailed) =	1.43688E-34
p-value	<.0001

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variable are related, for the purposes of establishing whether or not there exists a correlation between the implementing standards for compliance and implementing standards for certification.

The two variables in the hypothesis and the correlation test to be conducted are:

i) Implementing standards for compliance (X)

ii) Implementing standards for certification (Y)

The data collected for these two variables are nonparametric and the Spearman's Correlation technique will be used to test the null hypothesis (Siegel & Castellan, 1988). The data have been coded and ranked on the basis of their respective frequencies. The responses obtained from the survey were tabulated in MS Excel using pivot tables. The frequencies for variable (X) and (Y) were then ranked as per Spearmen Rank Technique independently from highest to lowest.

There were 100 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by (r). The Spearman's rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a relationship between two variables (Siegel & Castellan, 1998). A 95% confident interval (CI) was again used.

The closer r is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

The r value of 0.884, as obtained above, suggest a fairly strongly relationship between the two variables, that is implementing standards for compliance (X) and implementing standards for certification (Y) and the computed t-test derived at 18.796.

It is important for the researcher to report on the p-value, which is the probability of obtaining a value of the test statistic as extreme or more extreme, than actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

According Armitage & Berry (1994), the p-value and the confidence interval (CI) are computed around the observed proportion. The confidence interval utilised was 95%.

The p-value is the determining factor to accept or reject the null hypothesis. The p-value of 0.05 is the threshold used to evaluate the null hypothesis (iSixSigma, 2005). Researchers will reject a hypothesis with a p-value less

than 0.05, however according Dallas (2000), a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence against the null hypothesis. Should the p-value be close to zero, it signifies a false hypothesis (iSixSigma, 2005).

On the basis of the result of the p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used. It indicates that there is a direct correlation between implementing standards for compliance and implementing standards for certification.

5.7.1.3 **Testing correlation between the presence of a security policy and application of security policies**

The null hypothesis (Ho) being:

"There is no correlation between the presence of a security of a policy and the application of a security policy."

Test	**Pearson's Correlation**
Alternative hypothesis	**Presence of a security policy = Application of a security policy**
Performed by	**Tania Abrahams**
Numerator: Σ(xy)-N($\bar{x}$ $\bar{y}$) =	97
Denominator: $\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}$ =	184.9207939
Pearson's *r* = $r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}}$	0.524548905
R-squared =	0.275151554
t = $t = \frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$	6.099235704
Degrees of freedom =	98
Probability level (two-tailed) =	2.12209E-08
Probability level (one-tailed) =	1.06104E-08
p-value	<.0001

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variable are related, for the purposes of establishing whether or not there exists a correlation between the presence of a security policy and application of a security policy.

The two variables in the hypothesis and the correlation test to be conducted are:

i) Presence of a security policy (X)

ii) Application of a security policy (Y)

The data collected for these two variables are nonparametric and the Spearman's Correlation technique will be used to test the null hypothesis (Siegel & Castellan, 1988). The data have been coded and ranked on the basis of their respective frequencies. The responses obtained from the survey were tabulated in MS Excel using pivot tables. The frequencies for variable (X) and (Y) were then ranked as per Spearmen Rank Technique independently from highest to lowest.

There were 100 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by (r). The Spearman's rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a relationship between two variables (Siegel & Castellan, 1998). A 95% confident interval (CI) was again used.

The closer r is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

The r value of 0.524, as obtained above, suggest a fairly strongly relationship between the two variables, that is implementing standards for compliance (X) and implementing standards for certification (Y) and the computed t-test derived at 6.099.

It is important for the researcher to report on the p-value, which is the probability of obtaining a value of the test statistic as extreme or more extreme, than actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

According Armitage & Berry (1994), the p-value and the confidence interval (CI) are computed around the observed proportion. The confidence interval utilised was 95%.

The p-value is the determining factor to accept or reject the null hypothesis. The p-value of 0.05 is the threshold used to evaluate the null hypothesis (iSixSigma, 2005). Researchers will reject a hypothesis with a p-value less than 0.05, however according Dallas (2000), a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence

against the null hypothesis. Should the p-value be close to zero, it signifies a false hypothesis (iSixSigma, 2005).

On the basis of the result of the p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used, which indicates that there is a direct correlation between the presence of a security of a policy and the application of a security policy.

5.7.1.4 **Testing the correlation between clearly defined roles and responsibilities for the department and dedicated staff to manage IS.**

The null hypothesis (Ho) being:

"There is no correlation between clearly defined roles and responsibilities for the department and dedicated staff to manage IS."

Test	**Pearson's Correlation**
Alternative hypothesis	**Clearly defined roles and responsibilities for department = dedicated staff to manage IS**
Performed by	**Tania Abrahams**
Numerator: Σ(xy)-N($\bar{x}$ $\bar{y}$) =	296
Denominator: $\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}$ =	385.5629343
Pearson's *r* = $r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}}$	0.76770865
R-squared =	0.589376572
t = $t = \frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$	11.86007977
Degrees of freedom =	98
Probability level (two-tailed) =	1.19066E-20

Probability level (one-tailed) =	5.95332E-21
p-value	<.0001

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variable are related, for the purposes of establishing whether or not there exists a correlation between clearly defined roles and responsibilities and dedicated staff to manage IS within departments.

The two variables in the hypothesis and the correlation test to be conducted are:

i) Clearly defined roles and responsibilities (X)

ii) Dedicated staff to manage IS within departments (Y)

The data collected for these two variables are nonparametric and the Spearman's Correlation technique will be used to test the null hypothesis (Siegel & Castellan, 1988). The data have been coded and ranked on the basis of their respective frequencies. The responses obtained from the survey were tabulated in MS Excel using pivot tables. The frequencies for variable (X) and (Y) were then ranked as per Spearmen Rank Technique independently from highest to lowest.

There were 100 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by (r). The Spearman's rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a relationship between two variables (Siegel & Castellan, 1998). A 95% confident interval (CI) was again used.

The closer r is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

The r value of 0.767, as obtained above, suggest a fairly strongly relationship between the two variables, that is implementing standards for compliance (X) and implementing standards for certification (Y) and the computed t-test derived at 11.86.

It is important for the researcher to report on the p-value, which is the probability of obtaining a value of the test statistic as extreme or more extreme, than actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

According Armitage & Berry (1994), the p-value and the confidence interval (CI) are computed around the observed proportion. The confidence interval utilised was 95%.

The p-value is the determining factor to accept or reject the null hypothesis. The p-value of 0.05 is the threshold used to evaluate the null hypothesis (iSixSigma, 2005). Researchers will reject a hypothesis with a p-value less than 0.05, however according Dallas (2000), a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence against the null hypothesis. Should the p-value be close to zero, it signifies a false hypothesis (iSixSigma, 2005).

On the basis of the result of the p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used. It indicates that there is a direct correlation between clearly defined roles and responsibilities for the department and dedicated staff to manage IS.

5.7.1.5 **Testing correlation between an implemented information security awareness programme and staff regularly attends the programme**

The null hypothesis (Ho) being:

"There is no correlation between an implemented an information security awareness programme and staff regularly attends programme"

Test	**Pearson's Correlation**
Alternative hypothesis	**Response: Implemented and information security programme = staff regularly attends the programme**
Performed by	**Tania Abrahams**
Numerator: Σ(xy)-N($\bar{x}$ $\bar{y}$) =	296
Denominator: $\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}$ =	385.17
Pearson's *r* = $r = \frac{\sum xy - N\bar{x}\bar{y}}{\sqrt{\left(\sum x^2 - N\bar{x}^2\right)\left(\sum y^2 - N\bar{y}^2\right)}}$	0.768491835
R-squared =	0.5905797
t = $t = \frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$	11.88961
Degrees of freedom =	98
Probability level (two-tailed) =	1.03019E-20
Probability level (one-tailed) =	5.15095E-21
p-value	<.0001

Correlation test is being used for this case. It is a statistical technique which can show whether and how strongly pairs of variable are related, for the purposes of establishing whether or not there exists a correlation between an

implemented IS awareness programme and staff's regular attendance of the programme.

The two variables in the hypothesis and the correlation test to be conducted are:

i) Implemented IS awareness programme (X)

ii) Staff regularly attends the programme (Y)

The data collected for these two variables are nonparametric and the Spearman's Correlation technique will be used to test the null hypothesis (Siegel & Castellan, 1988). The data have been coded and ranked on the basis of their respective frequencies. The responses obtained from the survey were tabulated in MS Excel using pivot tables. The frequencies for variable (X) and (Y) were then ranked as per Spearmen Rank Technique independently from highest to lowest.

There were 100 cases (n) and a Spearman correlation coefficient was obtained for the two variables as given by (r). The Spearman's rank correlation coefficient is a technique which can be used to summarise the strength and direction (negative or positive) of a relationship between two variables (Siegel & Castellan, 1998). A 95% confident interval (CI) was again used.

The closer r is to +1 or -1, the stronger the likely correlation. A perfect positive correlation is +1 and a perfect negative correlation is -1 (Box & Jenkins, 1976).

The r value of 0.768, as obtained above, suggest a fairly strongly relationship between the two variables, that is implementing standards for compliance (X) and implementing standards for certification (Y) and the computed t-test derived at 11.88.

It is important for the researcher to report on the p-value, which is the probability of obtaining a value of the test statistic as extreme or more extreme, than actually obtained given that the tested null hypothesis is true (Daniel & Terrell, 1995).

According Armitage & Berry (1994), the p-value and the confidence interval (CI) are computed around the observed proportion. The confidence interval utilised was 95%.

The p-value is the determining factor to accept or reject the null hypothesis. The p-value of 0.05 is the threshold used to evaluate the null hypothesis (iSixSigma, 2005). Researchers will reject a hypothesis with a p-value less than 0.05, however according Dallas (2000), a small p-value is evidence against the null hypothesis while a large p-value means little or no evidence against the null hypothesis. Should the p-value be close to zero, it signifies a false hypothesis (iSixSigma, 2005).

On the basis of the result of the p-value (<0.0001) in the above test, the null hypothesis is unlikely to be true at the significance level used. It indicates that there is a direct correlation between an implemented security awareness programme and regular attendance of the programme by staff.

5.8 Areas where South Africa Excel

The public service in South Africa has made great strides in securing governments, which are attributed to the various mechanisms, international agreements, legislation and policy documents implemented. With the public service inherently dependant on the availability, integrity and confidentiality of it mission critical information, legislation that speaks to the preservation and protection of information is protected and preserved, are the Public Service Act, ECT Act, Copy Right Act and the MISS, which is a policy document.

Furthermore the various literatures reviewed related to governance, including aspects of ITG and ISG addresses the various aspects of compliance and the important factors that need to be taken into account during the enforcement process.

One of the benefits of BS7799/ISO17799 Standards (Human Level) highlights that employees will grow their knowledge, inculcate best practise and an organisational culture conscious of security will develop throughout the organisation on implementation of such standards. A positive for South Africa is note from the data analysed, that Senior Managers in the public service do have an increased awareness of threats against information as the respondents surveyed, the researcher concluded that 82% of the respondents strongly agreed that their departments have a great dependency on IT and

86% of the respondents concurred that they are concerned with information leaking as the department, employees and citizens would be most at risk.

According to Chang & Ho. (2006), Kankanhlli et. al (2003) the availability of financial resources is a managerial factor to ensure sufficient funding is available. Although a budget is allocated, overall the respondents indicated that they spend less than 10% of their annual budgets on IS to ensure the protection of information as an asset.

The literature reviewed on IS awareness, humans are perceived as the weakest link in the IS environment, however Barrett (2006) highlights that the strength of organisational cyber-defence is a knowledgeable workforce, therefore it is commendable that Senior management strongly agreed (50%) that IS is high on the agenda of their department and staff members receive IS awareness training on a regular basis, with 38% confirming quarterly. Although 62% of respondents confirmed that IS awareness programmes are compulsory to employees within their department, a significant 38% indicated that it is not compulsory. IS awareness programmes reviewed periodically, and this was confirmed by the respondents of whom 14% strongly agreed and 45% agreed. Overall the respondents, 18% strongly agreed and 27% agreed that staff receive regular updates on IS threats and staff is well aware of security topics ranging from e-mail and electronic communication, passwords, physical security, access to buildings, internet security, viruses, software licensing and copyright, clear desk policy, etc. In order of priority they have indicated that the following methods have proved most effective at raising IS levels; namely Induction (71%), Security Policy (67%) and letter of appointment (58%).

Security Policy is one of the ten fields of application of the ISO17799 (ISO/IEC17799), prescribing recommendations and guidelines of critical elements that should be in place to attain certification. The security policy provides guidelines and management advise for improving IS. From the population sampled and based on the MISS each department should have documented IS policies and 77% of the respondents surveyed indicated they

do have these policies in place. 46% of these senior managers indicated that they have dedicated staff to manage their IS and their roles and responsibilities are clearly defined. Access to information as an asset should be highly controlled and 40% strongly agreed, 48% agreed that their departments have appropriate physical and environmental security structures in place to safeguard areas that have ICT infrastructure and stores critical information. 54% indicated that they are able to locate all assets including software, hardware, staff and services used for information handling. Local and remote access to information assets is controlled. 32% of the departments do have business continuity plans in place in the event of a disaster ensuring a continuation of services should the latter occur.

Although the overall majority (71%) are aware of both BS and ISO standards, less than half of the populations surveyed indicated that their department has implemented these standards. The reason for implementation was either for certification or compliance.

5.9 Conclusion

In this chapter the researcher presented an analysis of the findings, results of the hypothesis tested and identified areas where South Africa excels. The finding gave a clear indication that the level of compliance with factors of ISM has room for significant improvement.

In the next chapter the researcher aims to draw conclusions and put forward recommendations specifying areas that require redress to ensure compliance with factors of ISM.

Chapter 6 – Conclusions and Recommendations

6.1 Introduction

In this last chapter of the research work, the researcher will summarise the research findings, present the conclusions and provides recommendations to the hypotheses formulated, in an attempt to answer the research questions.

The researcher identified that the increased usage of information and communication technologies in the public service have exposed and made the institution vulnerable to potential intrusions. Global trends indicate that Senior Managers are not implementing information security policies and procedures. Although policies and procedures exist for the secure control of information it is not known how high their awareness levels are to ensure the procedures are operationalised.

During the selection of the research topic, it was clear from the onset that value should be derived from the research to address areas where gaps were identified. The researcher deemed this as a motivating factor to undertake the challenge with the view to rise to the occasion.

The purpose of this research is to investigate factors of non-compliance of ISM in the public sector of South Africa. The increased usage of information and communication technologies in the public service have exposed and made the institution vulnerable to potential intrusions. Global trends indicate that Senior Managers are not implementing information security policies and procedures.

This chapter will thus highlight the main findings and draw conclusions with recommendations for future research work.

6.2 Conclusions of the study

The purpose of this research is to investigate factors of non-compliance of ISM in the public sector of South Africa. It is critical to ensure a culture of compliance with information security policies and procedures, thus minimising the risk associated with intrusions and the vulnerability of state information. With the advent of government developing a security framework, this research could make a meaningful contribution to that framework, as it would highlight areas that require immediate intervention with limited resources.

Implications

From the data analysed, one can note that Senior Managers in the public service do have an increased awareness of threats against information as the respondents surveyed, the researcher concluded that 82% of the respondents strongly agreed that their departments have a great dependency on IT and 86% of the respondents concurred that they are concerned with information leaking as the department, employees and citizens would be most at risk. Overall the respondents indicated that they spend less than 10% of their annual budgets on IS to ensure the protection of information as an asset.

Solms (2001) stated that an organisations increased dependency on technology, increases its vulnerability and costs with positive spin-offs as the creation of new opportunities. The typical implication is losing information as an asset, with severe and dire consequences for both the department, but more so for the citizen, whom the department is servicing. Policies based on best practise will ensure proper standards are followed, for the preservation of this asset and maintain the integrity of the department, and also further reducing possible threats the public service might encounter. As highlighted in the literature review, the South African public service has not been immune to such incidence as the Sasser virus, which hampered service delivery in 2003.

Senior Managers in the public service can curtail such risks by ensure that top management gives IS the attention it deserves. As highlighted in the King III Report on Good Governance, IS is a top management responsibility and prior to delegated this responsibility, due consideration should be given by Accounting Officers, who would ultimately be held liable for non-compliance.

Nosworthy (2000) highlighted that people, attitude, culture, education and training are key consideration when implementing IS.

Based on the analysis of the data Senior management strongly agreed (50%) that IS is high on the agenda of their department and staff members receive IS awareness training on a regular basis, with 38% confirming quarterly. Although 62% of respondents confirmed that IS awareness programmes are compulsory to employees within their department, a significant 38% indicated that it is not compulsory. IS awareness programmes reviewed periodically,

and this was confirmed by the respondents of whom 14% strongly agreed and 45% agreed. Overall the respondents, 18% strongly agreed and 27% agreed that staff receive regular updates on IS threats and staff is well aware of security topics ranging from e-mail and electronic communication, passwords, physical security, access to buildings, internet security, viruses, software licensing and copyright, clear desk policy, etc. In order of priority they have indicated that the following methods have proved most effective at rising IS levels; namely Induction (71%), Security Policy (67%) and letter of appointment (58%).

The implication is not having compulsory IS awareness training would have dire consequences for the public service as an institution. This could lead to increased risk exposure of the institution as a whole, making it vulnerable to intrusions by external parties. In addition security practitioners have a critical role to play, by increasing awareness of the current and prominent IS threats, thus compelling staff to more vigilant when utilising IT for service delivery.

Access to resources, such as sufficient budget is crucial to ensure the protection and preservation of assets through. The analysis of the data collected indicated that overwhelmingly 34% of respondents surveyed indicated that their IT budgets are R100,1m or more, whilst 72% of the respondents surveyed indicated they spend less than 10% of their annual budget on IS. Managerial factors include top management support and commitment, security education and training and regulations. Additional critical factors are awareness and financial resources (Chang & Ho, 2006; Kankanhlli et al. 2003). A change in practise for allocation of budget is an immediate solution to priorities IS in the public service. This will elevate the status of information as a critical asset to ensure the mechanisms are put in place to ensure preservation.

Risk Exposure

Individuals who handle this information play an important role and their behaviour towards IS will determine the level of risk and exposure. Behaviour and perception toward IS can be improved through continued awareness and training (Caralli and Wilson, 2003). As determined in the analysis of data, that

only 38% of respondents indicated that awareness training is compulsory is cause for concern.

According to Danchev (2003) IS awareness is critical to ensure full compliance with your organisation's IS policy. This can be attained through engaging employees, allowing them the opportunity to actively participate in the protection of information as an asset.

Changing the attitude, belief and making the public service a security conscious institution, would make significant contributions in reducing risks and entrenching best practise and principles to attain certification and compliance.

Impact

The challenge for achieving general goals of IS are the safeguarding of sensitive information, protection of the systems that host the information from potential loss, damage or destruction, providing assurances that the integrity, availability and confidentiality is not tainted and compliance and enforcement of legislation and regulatory frameworks to ensure the latter (Hong et al., Tudor, 2001.

Ngobeni & Grobler (2009) further affirms that the implementation of appropriate policy and enforcement of the latter will enable the protection; preservation of such information as an asset, which is the cornerstone of effectiveness. Without a policy a government department would not have a baseline to determine a consistent manner to control and monitor its environment, which would lead to inconsistencies and leave the department vulnerable to potential threats and intrusions by external parties.

The protection of information should be entrenched in an organisations' strategic objectives; and it is pertinent for the leadership to realise that the safekeeping of this asset is not just a technical aspect, but a business imperative (Solms and Solms, 2004). IS should not be viewed in isolation but holistically, taking into account the following elements, namely environment, legislation, personnel, technology, compliance and ethical considerations.

Certification creates access to global markets, protection of patents and the environment, government acquisition reforms and improves quality (Howie, 1995).

Compliance with information security best practise and ensuring implementation of policies as critical for the preservation and protecting the data within public service. It is thus pertinent for the public service as an institution to ensure that policies are established and fully implemented in relation all elements to ensure compliance. The implementation of proper systems, controls that would measure its effectiveness will ultimately lead to attaining an retaining compliance.

This process can succeed when driven by top management and implementing attendance of IS awareness training as part of the employees' performance management system, ensuring a culture that is IS conscious and assist with safeguarding assets.

Through regular audits, senior managers will be able to identify the gaps that require immediate attention for implementation.

To ensure compliance with the MISS it is critical that government should review practices to ensure policy objectives are met, international standards as a best practice is attained and increased awareness on IS by all employed in the public service to ensure the integrity, protection and preservation of information as an asset.

The MISS is not enough to ensure the protection of information as an asset. The researcher recommends the development of supporting procedures and guidelines for implementation across the public service. This will ensure a reference document is available for all employees.

Finance is a key resource to ensure information is protected and preserved at all cost. As indicated in Chapter 2 a study conducted in 2004 CSI/FBI Computer Crime and Security Survey highlighted that most organisations allocate between 1% and 5% of their IT budget to security. In this study it was found that overall less than 10% of the IT budget is spent on IS. By allocating more resources to this important asset the research would recommend that 15% is allocated as a standard practice across the public service spectrum. This will ensure the availability of sufficient resources to ensure the policy objectives are met.

38% of the respondents have indicated that IS awareness programme is not compulsory in their respective departments. By including this as a contractual obligation in the employment contract of employees, it would leave no room

for choice, thus ensuring that all public servants are participants in such programmes. These programmes should be reviewed at least twice per annum, however not withstanding that threats are evolving on a regular basis. Through the communication of security alerts from a central node, it will ensure that messages are disseminated through the public service, raising the awareness levels of pending threats.

Business continuity plans is crucial to ensure mission critical service will continue in the event of a disaster. Harsher measures should be put in place for departments that are not complying with this requirement.

6.3 Future Research

The present research was of limited scope thus not all the element of ISM could be addressed. Although the findings enlightens, ones perspective there are certain areas that require immediate attention to improve ISM in the public service. Thus the development of comprehensive security framework would be welcomed.

Another possible area of future research is to investigate a causal analysis of security breaches in the public service. This would prove valuable with the increase of insider threats on the escalation globally and the continuous drive for access to information.

As South Africa does not operate in vacuum and the availability of the internet has made earth smaller, another area of future research would be a comparative study of IS practise within SADC. This would greatly assist countries within the region to determine how they compare with neighbouring countries, but also afford the exchange of best practise from lessons learnt.

6.4 Recommendations

In general the following consideration could potentially enhance the level compliance with factors of ISM in the public service:

i) Top Management ownership, commitment, support and allocation of sufficient resources;

ii) The distribution and availability of a standardise IS training toolkit across the public service, that is compulsory and sustainable to ensure regular awareness training takes place;

iii) Change management interventions that would address attitude, belief and entrench an IS awareness culture within the public service;

iv) Incorporation of IS awareness as part of the performance management system in the public service;

7. List of References

Abu-Musa, A. A. (2005). “The Role of IT Governance in Improving Corporate Governance: A Proposed Model from Managerial Accounting Context” The Journal of Trade & Finance, The Scientific Journal of the Faculty of Commerce, Tanta University, Egypt Vol. 25.n 2, pp. 55-118.

Abu-Musa, A. A. (2006) “Evaluating the Security Controls of CAIS in Developing Countries: The Case of Saudi Arabia” The International Journal of Digital Accounting Research, Vol. 6, Iss. 11, pp. 25-64.

Aldhizer III, G. (2007). The Insider Threat. Internal Auditor, 65(2), 71-73.

Armitage, P., Berry, G., 1994. Statistical Methods in Medical Research (3rd ed.).

Band, D. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). *Comparing insider IT sabotage and Espionage: A Model based analysis*. Carnegie Mellon Software Engineering Institute Technical Report CMU/SEI 2006 TR 026.

Barrett, N. (2006), "Staff form strongest line of defence", *IT Week Magazine*, 27 March, p. 16.

Bingham, J. (2005), Intruders the biggest threat to network security, [Online], Available: http://www.networkworld.com/columnists/2005/022105faceoff-outsiders.html

Boote, D.N., & Beile, P. (2005). Scholars before researchers: On the centrality of the dissertation literature review in research preparation. Educational Researcher, 34(6), 3 – 15.

Brown, W. C. (2006). IT Governance, Architectural Competency, and the Vasa. Information management & Computer security, 140 – 154.

Cappelli, D., Desai, A., Moore, A., Shimeall, T., Weaver, E., Willke, B. (2006), "Management and education of the risk of insider threat (MERIT)", *Proceedings of the 24th International Systems Dynamics Conference, Nijmegen, The Netherlands*,.

Caralli, R. A., & Wilson, W. R. (2003). The challenges of security management. Carnegie-Mellon University. Software Engineering Institute. [Online]. Available: http://www.cert.org/archive/pdf/Esmchallenges.pdf [accessed 19 August 09]

Chang, S.E., and Ho, C.B., 2006 Organisational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, (106)3, pp. 345-361.

Cooper, D.R., & Schindler, P.S. (1998) Business Research Methods, Irwin McGraw-Hill

Cooper, D.R. & Schindler, P.S., (2003). Business Research Methods (8th Ed.) McGraw-Hill: New York

Corporate Governance Task Force. (2004). Information Security Governance – A Call to Action. National Cyber Security Summit Task Force.

Coulthard, A. & Vuori, T. (2002). Computer Viruses: A quantitative analysis. Logistics information management, vol 15, no. 5/6, pp400-409.

Crawford, K., Bosshardt, M. (1993), *Assessment of Position Factors that Increase Vulnerability to Espionage*, Defense Personnel Security Research Center, Monterey, CA,.

Crotty, M., (1998). The foundations of social research: meaning and perspective in the research process, London: SAGE

Cwele, S., (2009), State Security Minister's Budget Speech, [Online] http://www.pmg.org.za/briefing/20090701-state-security-ministers-budget-speech [Accessed: 30 July 2009]

Dagada, R., Eloff, M.M., Venter, L.M., (2009), Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?, ISSA

Dallal, G.E., (2000). Nonparametric Statistics.

Danchev, D. 2003, *Building and implementing a Successful Information Security Policy.* Windows Security resources for IT admin, Available from http://www.windowsecurity.com/pages/security-policy.pdf (Accessed 09 December 2009).

Daniel, W.W., & Terrel, J.C., 1995. Business Statistics for Management & Economics, (7th ed.), Houghton Mifflin Company, U.S.A.

De Haes, S., & Van Grembergen, W. (2008). Practices in IT Governance and Business/IT Alignment, Information Systems Control Journal, 2, 23 – 27.

Dodds, R., & Hague, I. (2004). Information Security – More than an IT issue? Chartered Accountants Journal, 56 – 57.

Draft Code of Governance Principles for South Africa, (2009), [Online] http://www.iodsa.co.za [Accessed: 19 August 2009]

Educational Resources Information Centre. (1982). ERIC processing manual (Section 5: Cataloging). Washington, DC.

Electric Light & Power, 84(4), 22-24.

ENISA, (2007), Information Security Awareness Initiatives: Current practice and the measurement of success, [Online] http://www.enisa.europa.eu [Accessed: 20 August 2009]

Enstrust. (2004) Information Security Governance (ISG): an essential element of corporate governance. [Online] Available: http://www.itresearch.forbes.com/detail/RES/1082396487_702.html

Ernst and Young (2004). Ernst and Young Global Information Security Survey 2004. [Online] http://www.ey.com [Accessed: 21 August 2009]

European Security Forum, 1991. Putting Security Awareness into perspective. [Online: http://home.sita.co.za/iss/awareness] [Accessed: 09 February 2010]

Federal Trade Commission. (2002). [Online]. Available: http://www.ftc.gov/opa/2004/10/factaidtheft.html

Federal Trade Commission. (2004). [Online]. Available: http://www.ftc.gov/opa/2004/10/factaidtheft.html

Fertell, D. (2003). Identity and the insider threat. US Banker, 113(5), 58.

Furnell, S., Phyo, A.H. (2003), "Considering the problem of insider IT misuse", Australian Journal of Information Systems, Vol. 10 No.2, pp.134-8.

Gall, M.D., Borg, W.R., & Gall, J.P. (1996). Education research: An introduction (6th ed.) White Plains, NY: Longman.

GASSP, 1995. International Information Security Foundation, Generally Accepted System Security Principles Committee.

Giacalone, R. (1987), "Reasons for employee sabotage in the workplace", *Journal of Business and Psychology*, Vol. 1 No.4, pp.367-78.

Goetz, J.P., & LeCompte, M.D. (1984). Ethnography and qualitative design in educational research. San Diego: Harcourt Brace Jovanovich.

Goodman, M. (2001) Making Computer Crime Count. United States Department of Justice Federal Bureau of Investigation Washington, the FBI Law Enforcement Bulletin

Goodwin, C.J. 2002. Research in Psychology Methods and Designs. 3rd Ed. New York: John Wiley and Sons, Inc.

Gordon, L., Loeb, M., Lucyshyn, W. & Richardson, R. (2005). Computer Crime and Security Survey. Computer Security Institute

Guant, N. 2000. Practical approaches to creating a security culture. International Journal of Medical Informatics, 60 (2), pp 151 – 157.

Guba, E.G., & Lincoln, Y.S. (1989). Fourth Generation Evaluation. Sage Publications.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. & Tatham, R.L. (2005). Multivariate data analysis (6th ed.) Upper Saddle River, NJ: Prentice Hall.
Herbig, K., Wiskoff, M. (2002), *Espionage Against the United States by American Citizens, 1947-2001*, Defense Personnel Security Research Center, Monterey, CA, .
Hart, C. (1998). Doing Literature Review: Releasing the social science research imagination. London: Sage.

Hong, K. S, Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243 – 448.

Howie. R.L. Jr. 1995. Competing through Standardisation. Business Week, October 18

ISACA, 2009. “Implementing and Continually Improving IT Governance.”

ISO/IEC 17799 Makes information assets even more secured. [Online] Available: http://www.iso.org/iso/en/commoncentre/pressreleases/2011/Ref963.html

ITGI. (2000). CobiT 3rd ed Framework.

Jones, B. R. (2007). Comment - virtual neighbourhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law & Criminology*, 97(2), 601-629.

Kalof, L., Dan, A. and Dietz, T. (2007) *Essentials of social research,* Open University Press.

Kirkpatrick, S. (2008). Refining Insider Threat Profiles. Security: For Buyers of Products, Systems & Services, 45(9), 56-63. Retrieved from Business Source Premier database.

Knapp, K., Marshall, T., Rainer, K., Ford, F. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No.4, pp.24-36.

Knowledgeleader. 2010. British Standard 7799 (ISO17799). [Online]. Available: http://www.knowledgeleader.com./iafreewebsite.nsf/content/SecurityBritishStandard7799 .

Kothari, C.R., 1985. Research Methodology Methods & Techniques, Wiley Eastern: New Delhi.

Krause, M., Tipton, H., 1999. Handbook of Information Security Management, Auerbach Publications.

Krone, T. (2005). Hacking Motives. High Tech Crime Brief, Canberra; Australia Institute of Criminology, Australian Government

LeCompte, M.D., Kilinger, J.K., Campbell, S.A., & Menke, D.W. (2003). Editor's introduction. Review of Educational Research, 73(2), 123 – 124.
Leedy, P.D., (1993). Practical Research: Planning and design (5th ed.). New York: MacMillan

Leedy, P.D., & Ormrod, J.E., (2005). Practical Research: Planning and Design, 8 th Edition. Pearson Merrill Prentice Hall

Malan, S., SABS ISO/IEC 17799: keeping on the safe side. Computer Business Review [online]. Available: http://www.cbr.co.za/news.aspx?pkl1NewsId=9279&pklCategoryID=391 [Accessed 20 August 2009]

Management Study Guide, 2011. Available: http://www.managementstudyguide.com/corporate-governance.htm [Accessed 09 November 2011]

March, N., (1996). Statistical Glossary

Mason, J., & Waywood, A. (1996). The role of theory in mathematics education and research. In A.J. Bishop, K. Clements, C. Keitel, J. Kilpatrick & C. Laborde (Eds.) International handbook of mathematics education (Netherlands: Kluwer Academic, 1055 – 1089.

Maxwell, J., (1996). Qualitative research design: An interactive approach. Thousand Oaks: SAGE

Microsoft Corporation, 2010, Microsoft Office Online [Online]. Available: http://office.microsoft.com/en-gb/FX010858001033.aspx [Accessed: 11 November 2010]

Miles, M.B., & Huberman, M.A. (1994). Qualitative Data Analysis: An Expanded Sourcebook (2nd ed.). Beverley Hills Sage.

Moulton, R., & Coles, R. (2003). Applying Information Security Governance. Computers and Security, 580 – 584.

Mouton, J. and Marais, H.C., (1996). Basic Concepts in Methodology of the Social Sciences. Pretoria: HSRC Publishers

Murphy, L., 2004. Survey preparation: Survey Sample & Response Rates.

Mustafi, C.K., Rao, S.S., 2003. Research Methodology for Managerial Decisions, Indian Institute of Management, Unique Press (P) Ltd.

Nceba, G. (1999). Computer Crime: Challenges of new technology. Nedbank ISS Crime Index, vol. 3, no 3. [Online]. Available: http://www.iss.co.za/Pubs/CRIMEINDEX/99VOL3NO4/Computer.html [Accessed: 22 August 2009]

Neuman, W.L., (2006), Social Research Methods: Qualitative and Quantitative Approaches, p149 – 374

NCES, 2005. Statistical Standards [Online]. Available: http://nces.ed.gov/ [Accessed: 12 November 2010]

Ngobeni, S.J. & Grobler, M.M., (2009), Information Security Policies for Governmental Organisations, the Minimum Criteria, Pretoria

Nosworthy, J. (2000). Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? *Computers and Security* 19(4): 337-347.

OECD. (2005). OECD Principles of Corporate Governance. OECD.

Olivier, M.S. (2004). Information Technology Research: A Practical Guide for Computer Science an Informatics. 2nd Ed. Van Schaik Publishers: Pretoria.

Ortega, R. (2006). the insider threat: when trusted assets go bad.

Petersen, R. (2004). Crafting Information Technology Governance. Information Systems Management, 7 – 22.

Pfleeger, C.P., 2000. Security in Computing, (2nd ed.) Prentice Hall.

Pipe, G. (2003, July). International Organizations Rally to Combat Cybercrime. I-Ways, p. 90.

Polity.org, (2006). Arrest, charges in hoax e-mail saga to be laid "very soon". [Online] http://www.polity.org.za/article/arrest-charges-in-hoax-email-saga-to-be-laid-very-soon [Accessed: 22 August 2009]

Posthumus, S. & Von Solms, R. (2004). A Framework for the Governance of Information Security. [Online] Available from: http://0-www.sciencedirect.com.innopac.wits.ac.za/science/article/pii/S0167404804002639

Raghuphati, W. (2007). Corporate Governance of IT: A Framework for Development. Communication of the ACM, 94 – 99.

RaoSoft, Inc. (2010). Sample Size Calculator [Online] Available from: http://www.roasoft.com/ [Accessed: 01 December 2010]

Reichel, M., & Ramey, M.A. (Eds.) (1987). Conceptual Frameworks for bibliographic education: Theory to Practice. Littleton Colorado: Libraries Unlimited Inc.

SABS, 2002. The Economic Benefits of a technical Regulatory Model in a Developing Country Context. Phase One Research Report – South Africa Bureau of Standards, Regulatory Affairs and Consumer Protection Division, July.

Saferpak, (2010). Surveys, Response Rate [Online]. Available: http://www.saferpak.com [Available: 02 December 2010]

Schneier, B., (2000). Secrets & Lies, Wiley-VCH Verlag GmbH.

Sepotokele, T., (2004). Computer virus hits public service, [Online] Available: http://www.iol.co.za/index.php?click_id=115&art_id=vn20040506025228479C666669&set_id=1 [accessed 19 August 09]

Shuttleworth, M., (2008). Validity and Reliability. [Online] http://www.experiment-resources.com/validity-and-reliability.html#ixzz0OwPKWwXD [Accessed: 22 August 2009]

Sieber, U. (1986). The International Handbook on Computer Crime, Great Britain, p4

Siegel, S., Castellan, N.J. (Jr)., (1988). Non-parametric Statistics for the Behavioural Sciences, (2nd ed.), New York.

Siponen, M.T. A conceptual foundation for organisational information security awareness. Information Management & Computer Security, Vol. 8, Issue 1, 2000, pp. 31-41.

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

Solms, S. H., (2001). Corporate governance and information security, Computers and Security, 20 (3), 215 – 218

Sophos.com (2004). South Africa government departments hit by Sasser. Virusinfo. Retrieved 10 February 2010, from http://www.sophos.com/virusinfo/articles/sasserza.html

South Africa, (2002). *Electronic Communications and Transactions Act, No 25 of 2002,* Republic of South Africa, Pretoria, available online at http://www.internet.org.za/ect act.html

South Africa, 1978: Copyright Act 98. Pretoria: Department of Trade and Industry

South Africa, 1997: Intellectual Property Laws amendment Act, Pretoria: Department of Trade and Industry

South Africa, 1994: Public Service Act, Pretoria, Department of Public Service and Administration.

Srikwan, S., Jokabsson, M. 2007. Using cartoons to teach Internet Security [online]. [Accessed 2009]. Available http://www.informatics.indiana.edu/markus/document/security-education.pdf

Steele, S. & Wargo C. (2007). Information Security Journal: A Global Perspective, Volume 16, 2007, pages 23 - 33

Stephanou, A.T. & Dagada, R, 2008. The impact of information security awareness training on information security behaviour: The case for further research. ISSA

Stiennon, R. (2006). Ignoring the insider threat. Network World, 23(33), 58.

Symantec, 2008. *Symantec report on the underground economy.*

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational Mechanisms for IT Governance. In W. Grembergen, Strategies for Information Technology Governance (pp. 1- 36). USA: Idea Group Publishing.

Von Solms, B. 2006. Information Security – The Fourth Wave. Computers and Security, 165 – 168.

Von Solms, B. 2005. Information Security Governance: CobIT or ISO 17799 or both? Computers and Security, 99 – 104.

Von Solms, R., & Von Solms, B. 2006. Information Security Governance: A Model Based on the Direct-Control Cycle. Computer and Security, 408 – 412.

Von Solms, R. 1998. Information Security Management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*. (6)5. pp.221-223.

Wallace, R., Lusthaus, A. & Kim, J. (2005). Computer Crimes, American Criminal Law Review, vol. 42. [Online]. Available: http://www.questia.com/PM.qst?a=o&se=gglsc&d=5009916521

Weill, P. 2004. IT Governance, How Top Performance Manage IT Decision Rights for Superior Results. Boston, Massachusetts: Harvard Business School Press.

Welman, J.C. & Kruger, S.J. 2004. Research Methodology. Oxford University Press. Oxford: New York.

Wilson, M., Hash, J. (2003), "Building an information technology security awareness and training program", US Department of Commerce, Washington, DC, NIST Special Publication 800-50.

Wixley, T., & Everingham, G. 2005. Corporate Governance 2nd ed. Cape Town, South Africa: Siber Ink CC.

Zikmund, W.G. (1997). Exploring marketing research (6th ed.) Fort Worth, TX: The Dryden Press.

Zuckermann, A., 1997. Using Standards as Barriers to Trade. New Steel, Mary 1997. pp 6-9.

Annexure A

Dear Sir / Madam

I am currently a post-graduate student at the University of Witwatersrand, studying towards my Masters in Management – Public Development Management. The title of my research report is Legal Aspects of Information Security in Public Sector in South Africa.

Attached find a copy of the survey questionnaire that would assist in determining my research questions,

- What are the implications?
- What is the general risk exposure?
- What could be the impact?
- What is the extent of deviation from these norms?

May I kindly request your participation in the survey which would take approximately 10 minutes of your time. I want to assure you that confidentiality will be maintained and all ethical considerations for the purposes of research will apply.

My contact details are (w) 021 4428547 or (c) 0833767305 for further enquiries.

Thank you

Tania Abrahams

Section 1

Position and departmental information

Please select the item that most applies to your department.

1. What is your position within the department?

- ☐ Head of Department
- ☐ Chief Information Officer
- ☐ IT Manager
- ☐ IT Security Manager
- ☐ IT Security Consultant
- ☐ IT Specialist
- ☐ Line of Business Manager

2. How many employees are employed in your department?

- ☐ 1 – 499
- ☐ 500 – 999
- ☐ 1000 – 1999
- ☐ 2000 – 2999
- ☐ 3000 – 3999
- ☐ 4000 – 4999
- ☐ > 5000

3. What is your departments' annual IT budget?

- ☐ R1m – R5m
- ☐ R5.1m – R10m
- ☐ R10.1m – R50m
- ☐ R50.1m to R100m
- ☐ R100.1m or more

4. What percentage of your IT budget is spent on information security?

   ☐ <10%

   ☐ 20% to 30%

   ☐ 31% to 40%

   ☐ 41% to 50%

   ☐ >51%

5. Our department is dependant on the usage of information technology.

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

   ☐ Strongly disagree

6. How many users have access internet access (this includes email, www and remote access).

   ☐ 1 – 99

   ☐ 100 – 499

   ☐ 500 – 999

   ☐ 1000 – 9999

   ☐ 10 000 – 49 999

   ☐ 50 000 and more

7. Do you use computer to store or handle sensitive information, such as:

   - ☐ Personal records
   - ☐ Customer records
   - ☐ Strategic and business plans
   - ☐ Financial records
   - ☐ Blue prints, formulas and inventions
   - ☐ Your own confidential information
   - ☐ Citizen/Customer confidential information

8. Are you concerned about confidential information leaking out of your department?

   - ☐ Yes
   - ☐ no

9. If the confidentiality of the information or the information entrusted in your care is compromised, who is most at risk?

   - ☐ The department
   - ☐ Employees
   - ☐ Citizens

10. Information security is important to our department?

    - ☐ Strongly agree
    - ☐ Agree
    - ☐ Neutral
    - ☐ Disagree
    - ☐ Strongly disagree

Section 2
Governance and Information Security Standards

1. Does your organisation have dedicated staff to manage information security?

   ☐ Yes

   ☐ No
2. Do you have a documented information security policy?

   ☐ Yes

   ☐ No

3. Are the roles and responsibilities for information security in your department well defined?

   ☐ Yes

   ☐ No

4. Do you have appropriate physical and environmental security structures to safeguard areas that have ICT infrastructure that stores information?

   ☐ Yes

   ☐ No
5. Can you identify and locate all assets (including software, hardware, staff and services) used for information handling?

   ☐ Yes

   ☐ No

6. Is local and remote access to your information assets adequately controlled?

   ☐ Yes

   ☐ No

7. All security beaches or suspected breaches are reported.

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

   ☐ Strongly disagree

8. We have a business continuity plan, which addresses the protection of critical business information to ensure continuity in the event of a disaster.

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

   ☐ Strongly disagree

9. Are you aware of the information security standard ISO17799:2000 and BS7799?

   ☐ Yes

   ☐ No

10. Have you implemented the standard?

    ☐ Yes

    ☐ No

11. We have implemented the standard for

    ☐ compliance

    ☐ certification

Section 3

Information Security Awareness

Please select the item that most applies to your department.

1. Our department have implemented an information security awareness programme.

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

   ☐ Strongly disagree

2. We frequently conduct information security awareness training

   ☐ Annually

   ☐ Quarterly

   ☐ Bi-annually

3. Our information security awareness programme is compulsory for all employees

   ☐ Yes

   ☐ No

000000End00000